Rekisterinpitäjän osoitusvelvollisuus EU:n yleisessä tietosuoja-asetuksessa

Helsingin yliopisto
Oikeustieteellinen tiedekunta
Pro gradu -tutkielma
Tammikuu 2018
Viestintä- ja informaatio-oikeus
Tekijä: Sonja Vainio
Ohjaaja: Päivi Korpisaari

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Tiedekunta/Osasto - Fakultet/Sektion – Faculty Oikeustieteellinen tiedekunta		Laitos - Institution – Department
Tekijä - Författare – Author Sonja Vainio		
Työn nimi - Arbetets titel – Title Rekisterinpitäjän osoitusvelvollisuus EU:n yleisessä tietosuoja-asetuksessa		
Oppiaine - Läroämne – Subject Viestintä- ja informaatio-oikeus		
Työn laji - Arbetets art – Level Pro gradu -tutkielma	Aika - Datum – Month and year Tammikuu 2018	Sivumäärä - Sidoantal – Number of pages XV + 66

Tiivistelmä - Referat – Abstract

Euroopan unionin yleinen tietosuoja-asetus (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta) tuo keskeisiä muutoksia henkilötietojen käsittelyyn niin jäsenvaltoissa kuin kansainvälisestikin.

Yksi näistä muutoksista on osoitusvelvollisuus, jolla rekisterinpitäjät velvoitetaan osoittamaan noudattavansa käsittelytoiminnassaan tietosuojalainsäädännön velvoitteita. Tutkielman aiheena on rekisterinpitäjän osoitusvelvollisuus EU:n yleisessä tietosuoja-asetuksessa. Osoitusvelvollisuus ei konseptina ole täysin uusi, mutta EU:n tietosuojauudistuksen myötä se on tuotu ensimmäistä kertaa osaksi EU:n tietosuojalainsäädäntöä. Tutkielmassa perehdytään osoitusvelvollisuuteen EU:n tietosuoja-asetuksen keinona toteuttaa henkilötietojen suojaa. Tutkielman tarkoituksena on tarkastella, mitä osoitusvelvollisuudella tarkoitetaan, sekä mitä keskeisiä vaatimuksia velvoite asettaa rekisterinpitäjälle.

Tutkielmassa tarkastellaan ja kontekstualisoidaan osoitusvelvollisuutta EU:n yleisessä tietosuoja-asetuksessa. Erityisesti käsitellään lainsäädäntöuudistuksen tavoitteiden heijastumista osoitusvelvollisuuden sisältöön, laajuuteen ja luonteeseen, sekä viitekehystä sille, miksi osoitusvelvollisuus otettiin juuri nyt osaksi tietosuojalainsäädäntöä, eli mihin lainsäädäntötarpeeseen osoitusvelvollisuus vastaa. Lisäksi tutkielman oleellisena tutkimuskysymyksenä on osoitusvelvollisuuden sisällön ja erityispiirteiden tarkastelu. Keskeistä on selvittää, mitä osoitusvelvollisuudella tarkoitetaan ja mitä vuorovaikutussuhteita se luo.

Tutkielmassa tarkastellaan myös osoitusvelvollisuuden laajuutta ja kohdistumista tietosuoja-asetuksessa sekä keskeisiä keinoja, joilla rekisterinpitäjä voi toteuttaa osoitusvelvollisuutta. Rekisterinpitäjille osoitusvelvollisuus merkitsee uutta haastetta, ja velvoitteen käytännön toteuttamiskeinot on pääosin jätetty rekisterinpitäjän valittavaksi. Tutkielmassa tarkastellaan keskeisiä tietosuojahallinnollisia käytäntöjä, jotka voidaan ottaa osaksi osoitusvelvollisuuden täyttämistä.

Kokonaisuutena tietosuoja-asetuksen rekisterinpitäjiä koskeva osoitusvelvollisuus on verrattain uusi ja täsmentymätön velvoite. On kuitenkin ilmeistä, että rekisterinpitäjän vastuu käsittelyn lainmukaisuudesta varmistumisesta korostuu osoitusvelvollisuuden myötä. Toisaalta osoitusvelvollisuus on laadittu skaalautuvaksi ja jättää rekisterinpitäjälle harkintavaltaa niistä keinoista, joilla rekisterinpitäjä varmistaa henkilötietojen suojan tehokkaan toteutumisen toiminnassaan. Jos osoitusvelvollisuudesta mukautuu tietosuojauudistuksessa tavoiteltu joustava keino, saattaa velvollisuus johtaa rekisterinpitäjän parempaan ymmärrykseen omasta toiminnasta sekä tehokkaampaan henkilötietojen suojaan käytännössä.

Avainsanat – Nyckelord – Keywords
tietosuoja – EU:n yleinen tietosuoja-asetus – osoitusvelvollisuus

Säilytyspaikka – Förvaringställe – Where deposited

Muita tietoja – Övriga uppgifter – Additional information

LÄHTEET

Kirjallisuus ja artikkelit

Albers, Marion: Realizing the complexity of data protection. Teoksessa *De Hert, Paul — Gutwirth, Serge:* Reloading Data Protection. Springer Netherlands, 2014, s. 213-235. (Albers 2014).

Albrecht, Jan Philipp: How the GDPR Will Change the World. European Data Protection Law Review, Vol 2, Issue 3. 2016, s. 287–289. (Albrecht 2016).

Alhadeff, Joseph — Van Alsenoy, Brendan — Dumortier, Jon: The accountability principle in data protection regulation: origin, development and future directions. Teoksessa *Ilten, Carla — Kroener, Inga — Neyland, Daniel — Postigo, Hector:* Managing Privacy through Accountability. Palgrave Macmillan UK, 2012, s. 49-82. (Alhadeff — Van Alsenoy — Dumortier 2012).

Barnard-Wills, David: The technology foresight activities of European Union data protection authorities. Technological Forecasting and Social Change, Volume 116, 2017, s. 142-150. (Barnard-Wills 2017).

Bennett, Colin: Regulating privacy: Data protection and public policy in Europe and the United States. Cornell University Press, 1992. (Bennett 1992).

Bennett, Colin: International privacy standards: can accountability be adequate? Privacy Laws and Business International, Vol. 106, 2010, s. 21-23. (Bennett 2010).

Bennett, Colin: The accountability approach to privacy and data protection: assumptions and caveats. Teoksessa *Ilten, Carla — Kroener, Inga — Neyland, Daniel — Postigo, Hector:* Managing Privacy through Accountability. Palgrave Macmillan UK, 2012, s. 33-48. (Bennett 2012).

Bräutigram, Tobias: Getting High on Information? The European Commission's Proposal for Renewal of the Data Protection Legislation. JFT 5/2012, s. 415-435. (Bräutigam 2012).

Butin, Denis — Chicote, Marcos — Le Métayer, Daniel: Strong accountability: beyond vague promises. Teoksessa De Hert, Paul — Gutwirth, Serge: Reloading Data Protection. Springer Netherlands, 2014, s. 343-369. (Butin — Chicote — Le Métayer 2014).

Butin, Denis — Le Métayer, Daniel: A guide to end-to-end privacy accountability. Proceedings of the First International Workshop on Technical and Legal Aspects of Data Privacy. IEEE Press, 2015. (Butin — Le Métayer 2015).

Bygrave, Lee Andrew: Data Privacy Law: An International Perspective. Oxford University Press, 2014. (Bygrave 2014).

Carey, Peter: Data protection: a practical guide to UK and EU law. Oxford University Press, 2015. (Carey 2015).

Cavoukian, Ann — Taylor, Scott — Abrams, Martin E: Privacy by Design: essential for organizational accountability and strong business practices. Identity in the Information Society 3.2, 2010, s. 405-413. (Cavoukian - Taylor - Abrams 2010).

Coudert, Fanny: Accountable Surveillance Practices: Is the EU Moving in the Right Direction? Annual Privacy Forum, Springer, 2014. (Coudert 2014).

Davies, Simon: The Data Protection Regulation: A Triumph of Pragmatism over Principle? European Data Protection Law Review, Volume 2, Issue 3 (2016), s. 290-296. (Davies 2016).

De Hert, Paul — Gutwirth, Serge: Data protection in the case law of Strasbourg and Luxembourg: Constitutionalisation in action. Teoksessa *Gutwirth, Serge — Poullet, Yves — De Hert, Paul — de Terwangne, Cécile — Nouwt, Sjaak* (toim.)*:* Reinventing Data Protection? Springer Netherlands, 2009, s. 3-44. (De Hert — Gutwirth 2009).

De Hert, Paul — Papakonstantinou, Vagelis: The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. Computer Law & Security Review 28.2 (2012), s. 130-142. (De Hert — Papakonstantinou 2009).

De Hert, Paul: From the Principle of Accountability to System Responsibility – Key Concepts in Data Protection Law and Human Rights Law discussions. In International Data Protection Conference 2011, s. 88-120. Hungarian Official Journal Publisher. (De Hert 2011).

De Hert, Paul: Accountability and system responsibility: New concepts in data protection law and human rights law. Teoksessa *Ilten, Carla — Kroener, Inga — Neyland, Daniel — Postigo, Hector:* Managing Privacy through Accountability. Palgrave Macmillan UK, 2012, s. 193-232. (De Hert 2012).

De Hert, Paul — Papakonstantinou, Vagelis — Wright, David — Gutwirth, Serge: The proposed Regulation and the construction of a principles-driven system for individual data protection. Innovation: The European Journal of Social Science Research, 26(1-2), s. 133-144. (De Hert ym. 2013).

De Hert, Paul — Papakonstantinou, Vagelis: The new General Data Protection Regulation: Still a sound system for the protection of individuals? Computer Law & Security Review, *32*(2), s. 179-194, 2016. (De Hert — Papakonstantinou 2016).

Foegle, Jean-Philippe: Chronique du droit «Post-Snowden»: La CJUE et la CEDH sonnent le glas de la surveillance de masse. Protection des données personnelles (CEDH et CDFUE). La Revue des droits de l'homme. Revue du Centre de recherches et d'études sur les droits fondamentaux 2016. (Foegle 2016).

González-Fuster, Gloria: The Emergence of Personal Data Protection as a Fundamental Right of the EU. Springer International Publishing, 2014. (González-Fuster 2014).

Greenleaf, Graham: Data Protection in a globalised network. Teoksessa *Brown, Ian:* Research Handbook on Governance of the Internet. Edward Elgar Publishing Ltd, 2013. (Greenleaf 2013).

Hildebrandt, Mireille — Tielemans, Laura: Data protection by design and technology neutral law. Computer Law & Security Review, Volume 29, Issue 5, 2013, s. 516. (Hildebrandt — Tielemans 2013).

Hirvonen, Ari: Mitkä metodit? Opas oikeustieteen metodologiaan. Yleisen oikeustieteen julkaisuja 17. Helsinki 2011. (Hirvonen 2011)

Lindroos-Hovinheimo, Susanna: Elämäntarinoiden hallintaa – eurooppalainen henkilötietojen suoja yksilöllistymisen ilmentäjänä. Teoksessa *Korpisaari, Päivi* (toim.): Oikeus, tieto ja viesti. Viestintäoikeuden vuosikirja 2015. (Lindroos-Hovinheimo 2016).

Huuskonen, Mikko: Oikeustieteellisen tutkimuksen rooli suhteessa tekijänoikeuspolitiikkaan. Oikeus 2007 (36); 4: s. 434-437. (Huuskonen 2007).

Kallasvuo, Karoliina: Omadata ja oikeus siirtää tiedot järjestelmästä toiseen. Teoksessa *Korpisaari, Päivi* (toim.): Oikeus, tieto ja viesti. Viestintäoikeuden vuosikirja 2015. (Kallasvuo 2016).

Karhula, Päivikki: Sähköpaimen - kansalainen ubiikkiyhteiskunnan varjossa. Teoksessa *Karhula, Päivikki* (toim.): Paratiisi vai panoptikon? Näkökulmia ubiikkiyhteiskuntaan. Eduskunnan kirjaston tutkimuksia ja selvityksiä 10. Eduskunnan kirjasto, 2008. (Karhula 2008).

Keinänen, Anssi: Mitkä tekijät vaikuttavat yritysten halukkuuteen noudattaa sääntelyä ja miten noudattamista voitaisiin parantaa? Teoksessa *Keinänen, Anssi — Kukkonen, Reima — Kilpeläinen, Mia* (toim.): Oikeustieteiden moniottelija - Matti Tolvanen 60 vuotta. Edita Publishing Oy, 2016. (Keinänen 2016).

Kiss, Attila — Szőke, Gergely László: Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation. Teoksessa *Gutwirth, Serge — Leenes, Ronald — de Hert, Paul* (toim.): Reforming European Data Protection Law. Law, Governance and Technology Series, vol 20. Springer, Dordrecht, 2015. (Kiss — Szőke 2015).

Koillinen, Mikael: Henkilötietojen suoja itsenäisenä perusoikeutena. Oikeus 2013/2, 15.6.2013. Referee-artikkeli. (Koillinen 2013).

Koillinen, Mikael: Hallinnolliset seuraamukset tietosuojan sanktiomekanismina. Defensor Legis 2016/4, s. 570, 6.10.2016. (Koillinen 2016).

Koops, Bert-Jaap: The trouble with European data protection law. International Data Privacy Law, Volume 4, Issue 4, 1 November 2014, s. 250–261. (Koops 2014).

Korhonen, Rauno: Perusrekisterit ja tietosuoja. Edita Publishing Oy, 2003. (Korhonen 2003).

Korhonen, Rauno: Informaatio-oikeuden asemasta oikeuksien kentässä. Teoksessa: *Mäkelä, Sauli* (toim.): Oikeusteorian poluilla. Juhlakirja professori Rauno Halttunen. Lapin yliopiston oikeustieteellisiä julkaisuja, sarja c 42. Rovaniemi, 2006. (Korhonen 2006).

Korpisaari, Päivi: Oikeudenalan tunnusmerkeistä ja oikeudenalajaotuksen tarpeellisuudesta. Lakimies 7-8/2015, s. 987-1004. (Korpisaari 2015).

Koski, Saara: Lasten henkilötietojen suojan tehokkuus ja riittävyys Euroopan Unionissa – erityisesti esineiden internetin sovelluksissa. Teoksessa *Korpisaari, Päivi* (toim.): Viestinnän muuttuva sääntely. Viestintäoikeuden vuosikirja 2016, 31.12.2016. Referee-artikkeli. (Koski 2017).

Kranenborg, Herke: Article 8 Protection of Personal Data. Teoksessa *Peers, Steve ym.* (toim.): The EU Charter of Fundamental Rights. A commentary. Hart Publishing, 2014. (Kranenborg 2014).

Matzner, Tobias — Masur, Philipp K. — Ochs, Carsten, — von Pape, Thilo: Do-It-Yourself Data Protection—Empowerment or Burden? Teoksessa *Gutwirth, Serge — Leenes, Ronald — de Hert, Paul:* Data protection on the move, 2016, s. 277-305. Springer Netherlands, 2016. (Matzner ym. 2016).

Mayer-Schönberger, Viktor — Cukier, Kenneth: Big Data. A revolution that will transform how we live, work and think. John Murray, 2013. (Mayer-Schönberger — Cukier 2013).

Mikkonen, Tomi: Perceptions of controllers on EU data protection reform: A Finnish perspective. Computer Law & Security Review, Volume 30, Issue 2, 2014, s. 190-195. (Mikkonen 2014).

Mouzakiti, Foivi: Transborder Data Flows 2.0: Mending the Holes of the Data Protection Directive. European Data Protection Law Review, Volume 1, Issue 1, 2015, s. 39-51. (Mouzakiti 2015).

Partanen, Heikki: Kansallinen tietosuojapolitiikka ja EU:n tietosuoja-asetus. Teoksessa *Korpisaari, Päivi:* Viestintäoikeus nyt: viestintäoikeuden vuosikirja 2014. Helsingin yliopiston oikeustieteellinen tiedekunta, 2015, s. 162-173. (Partanen 2015).

Pitkänen, Olli — Tiilikka, Päivi — Warma, Eija: Henkilötietojen suoja. Alma Talent, 2014. (Pitkänen — Tiilikka — Warma 2014).

Raab, Charles: The Meaning of 'Accountability' in the Information Privacy Context. Teoksessa *Ilten, Carla — Kroener, Inga — Neyland, Daniel — Postigo, Hector:* Managing Privacy through Accountability. Palgrave Macmillan UK, 2012, s. 15-32. (Raab 2012).

Ratsula, Niina: Compliance. Eettinen ja vastuullinen liiketoiminta. Talentum Pro, 2016. (Ratsula 2016).

Saarenpää, Ahti: Oikeuden valtatie ja arkipäivän perusoikeudet. Teoksessa *Aarto, Markus – Vartiainen, Markku* (toim.): Oikeus kansainvälisessä maailmassa : Ilkka Saraviidan juhlakirja. Edita, 2008, s. 135-146. (Saarenpää 2008).

Saarenpää, Ahti: Henkilö- ja persoonallisuusoikeus. Teoksessa *Tammilehto, Timo* (toim.): Oikeusjärjestys, osa 1. Lapin yliopisto, 2012. (Saarenpää 2012).

Van Hoecke, Mark — Dhont, Jan: Obstacles and opportunities for the harmonisation of law in Europe: The case of privacy. Teoksessa *Heiskanen, Veijo — Kulovesi, Kati* (toim.): Function and future of European law. Publications of the Faculty of Law, University of Helsinki, 1999. (Van Hoecke — Dhont 1999).

Tala, Jyrki: Lakien laadinta ja vaikutukset. Edita Publishing Oy, 2005. (Tala 2005).

Tzanou, Maria: The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance. Bloomsbury Publishing, 2017. (Tzanou 2017).

Wallin, Anna-Riitta: Tiedonsaanti asiakirjoista ja henkilötietojen suoja EU:n perusoikeuskirjassa tunnustettuina perusoikeuksina. Teoksessa *Nieminen, Liisa* (toim.): Perusoikeudet EU:ssa. Lakimiesliiton Kustannus, 2001. (Wallin 2001).

Vanto, Jarno: Henkilötietolaki käytännössä. Lakitieto, 2003. (Vanto 2003).

Virallislähteet

Euroopan komissio

KOM(2010) 245 lopullinen: Euroopan digitaalistrategia. Bryssel, 19.5.2010. (KOM(2010) 245).

KOM (2010) 609: Kattava lähestymistapa henkilötietojen suojaan Euroopan unionissa. Bryssel, 4.11.2010. (KOM(2010) 609).

KOM(2012) 9 lopullinen: Yksityisyydensuoja verkottuvassa maailmassa–Euroopan uusi tietosuojakehys. Bryssel, 25.1.2012 . (KOM(2012) 9).

OECD

OECD 2013a, s. 97: The OECD Privacy Framework. 2013. (OECD 2013a). Saatavissa: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [Tieto haettu 1.1.2018]

Tietosuojatyöryhmä (“Article 29 Working Party”)

WP 105

Article 29 Data Protection Working Party: Working document on data protection issues related to RFID technology. 10107/05/EN, WP 105, 19.1.2005.

WP 136

Article 29 Data Protection Working Party: Opinion 4/2007 on the concept of personal data. 01248/07/EN, WP 136, 20.6.2007.

WP 168

Article 29 Data Protection Working Party: The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. 02356/09/EN, WP 168, 1.12.2009.

WP 169

Article 29 Data Protection Working Party: Opinion 1/2010 on the concepts of "controller" and "processor". 00264/10/EN, WP 169, 16.2.2010.

WP 173

Article 29 Data Protection Working Party: Opinion 3/2010 on the principle of accountability. 00062/10/EN, WP 173, 13.7.2010.

WP 179

Article 29 Data Protection Working Party: Opinion 8/2010 on applicable law. 0836-02/10/EN, WP 179, 16.12.2010.

WP 187

Article 29 Data Protection Working Party: Opinion 15/2011 on the definition of consent. 01197/11/EN, WP 187, 13.7.2011.

WP 191

Article 29 Data Protection Working Party: Opinion 01/2012 on the data protection reform proposals. 00530/12/EN, WP 191, 23.3.2012.

WP 202

Article 29 Data Protection Working Party: Opinion 02/2013 on apps on smart devices. 00461/13/EN, WP 202, 27.2.2013.

WP 203

Article 29 Data Protection Working Party: Opinion 3/2013 on purpose limitation. 00569/13/EN, WP 203, 2.4.2013.

WP 216

Article 29 Data Protection Working Party: Opinion 05/2014 on Anonymisation Techniques. 0829/14/EN, WP 216, 10.4.2014.

WP 217

Article 29 Data Proteciton Working Party: Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. WP 217, 9.4.2014.

WP 223

Article 29 Data Proteciton Working Party: Opinion 8/2014 on the Recent Developments on the Internet of Things. 14/EN, WP 233, 16.9.2014.

WP 243

Article 29 Data Proteciton Working Party: Guidelines on Data Protection Officers (‘DPOs’). 16/EN,WP 243, 13.12.2016.

WP 248

Article 29 Data Proteciton Working Party: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. 17/EN, WP 248, 4.4.2017.

WP 259

Article 29 Data Proteciton Working Party: Guidelines on Consent under Regulation 2016/679. 17/EN, WP 259, 28.11.2017.

WP 260

Article 29 Data Proteciton Working Party: Guidelines on transparency under Regulation 2016/679. 17/EN, WP 260, 28.11.2017.

WP29 kirjelmäliite

Liite WP 29:n kirjelmille trilogin yhteydessä 17.6.2015 http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf [Tieto haettu 1.1.2018]

Oikeuskäytäntö

Euroopan ihmisoikeustuomioistuin

Leander v. Ruotsi

A-sarja nro 116. Leander v. Ruotsi. Annettu 26.3.1987.

I. v. Suomi

Asia 20511/03 I. v. Suomi. Annettu 17.7.2008.

S. ja Marper v. Yhdistynyt kuningaskunta

Yhdistetyt asiat 30562/04 ja 30566/04 S. ja Marper v. Yhdistynyt kuningaskunta. Annettu 4.12.2008. Julkaistu vuosikirjassa 2008.

Euroopan unionin tuomioistuin

Asia C-101/01

Asia C-101/01 Rikosoikeudenkäynti vastaan Bodil Lindqvist. Annettu 6.11.2003.

Asia C-275/06

Asia C-275/06 Productores de Música de España (Promusicae) vastaan Telefónica de España SAU. Annettu 29.1.2008.

Asia C-73/07

Asia C-73/07 Tietosuojavaltuutettu vastaan Satakunnan Markkinapörssi Oy ja Satamedia Oy. Annettu 16.12.2008.

Asia C-553/07

Asia C-553/07 College van burgemeester en wethouders van Rotterdam vastaan M. E. E. Rijkeboer. Annettu 7.5.2009.

Asia C-360/10

Asia C-360/10 Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) vastaan Netlog NV. Annettu 16.2.2012.

Asia C-416/10

Asia C-416/10 Jozef Križan ym. vastaan Slovenská inšpekcia životného prostredia. Annettu 15.1.2013.

Asia C-131/12
Asia C-131/12 Google Spain SL ja Google Inc. vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González. Annettu 13.4.2014.

Asia C-212/13
Asia C-212/13 František Ryneš v. Úřad pro ochranu osobních údajů. Annettu 11.12.2014.

Asia C-615/13
Asia C-615/13 ClientEarth ja Pesticide Action Network Europe (PAN Europe) vastaan Euroopan elintarviketurvallisuusviranomainen. Annettu 16.7.2015.

Asia C-230/14
Asia C-230/14 Weltimmo s.r.o. vastaan Nemzeti Adatvédelmi és Információszabadság Hatóság. Annettu 1.10.2015.

Asia C-362/14
Asia C-362/14 Maximillian Schrems vastaan Data Protection Commissioner. Annettu 6.10.2014.

Asia C-191/15
Asia C-191/15 Verein für Konsumenteninformation vastaan Amazon EU Sàrl. Annettu 28.7.2016.

Asia C-210/16
Asia C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein vastaan Wirtschaftsakademie Schleswig-Holstein GmbH, muina osapuolina Facebook Ireland Ltd ja Vertreter des Bundesinteresses beim Bundesverwaltungsgericht. Julkisasiamiehen ratkaisuehdotus annettu 24.10.2017.

Muut lähteet

Accountability projects

Centre for Information Policy Leadership as Secretariat to the Galway Project: Data Protection Accountability: The Essential Elements. A document for Discussion. 2009. (Centre for Information Policy Leadership 2009).

Centre for Information Policy Leadership, Secretariat to the Paris Project: Demonstrating and Measuring Accountability. A Discussion Document. Accountability Phase II – The Paris Project. 2010. (Centre for Information Policy Leadership 2010).

Tutkimukset ja raportit

VAHTI-raportti 2016: Valtiovarainministeriö: EU-tietosuojan kokonaisuudistus. VAHTI-raportti - 7/2016. (VAHTI-raportti 2016)

Valtioneuvoston selvitys- ja tutkimustoiminta, Policy Brief 10/2017, Enroth, Timo — Neuvonen, Riku: EU:n tietosuoja-asetuksen yritysvaikutukset. Saatavilla: http://tietokayttoon.fi/documents/1927382/2116852/10_2017_+EUn+tietosuoja-asetuksen+yritysvaikutukset/7f043abc-2068-45f2-8470-0b2df19f7189?version=1.0 (VN 2017). [Tieto haettu 1.1.2018].

Oikeusministeriö: EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö. Oikeusministeriön mietintöjä ja lausuntoja 35/2017. (TATTI-mietintö).

Verkkolähteet

Aarnio, Reijo: Tietosuoja-asetuksen tulkinta ja tulevat ohjeet. Tietosuojavaltuutetun blogi. 30.6.2017.
Saatavilla: http://tietosuoja.fi/fi/index/blogi/6IUtCELFH/2017/FPFZTnPN9.html.stx (Aarnio 2017) [Tieto haettu 1.1.2018].

Buttarelli, Giovanni: Hitting the ground running: How regulators and businesses can really put data protection accountability into practice. Puhe European Data Protection Days (EDPD) -konferenssissa Berliinissä, 15.5.2017. Saatavilla: https://edps.europa.eu/sites/edp/files/publication/17-05-15_edpd_keynote_speech_en_0.pdf (Buttarelli 2017). [Tieto haettu 1.1.2018].

Centre for Information Policy Leadership as Secretariat to the Galway Project: Data Protection Accountability: The Essential Elements. A document for Discussion. 2009. (Centre for Information Policy Leadership 2009).

Centre for Information Policy Leadership, Secretariat to the Paris Project: Demonstrating and Measuring Accountability. A Discussion Document. Accountability Phase II – The Paris Project. 2010. (Centre for Information Policy Leadership 2010).

The Guardian: Lawyer suing Facebook overwhelmed with support
Saatavilla: https://www.theguardian.com/technology/2014/aug/06/facebook-privacy-action-austria-max-schrems (Guardian 2014). [Tieto haettu 1.1.2018].

Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali
Saatavilla: http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali (Garante 2017). [Tieto haettu 1.1.2018].

Information Commissioner's Office blog: GDPR is an evolution in data protection, not a burdensome revolution, Posted on August 25, 2017.
Saatavilla: https://iconewsblog.org.uk/2017/08/25/gdpr-is-an-evolution-in-data-protection-not-a-burdensome-revolution/ (ICO 20171). [Tieto haettu 1.1.2018].

Information Commissioner's Office: Guidance: what to expect and when
Saatavilla: https://ico.org.uk/for-organisations/data-protection-reform/guidance-what-to-expect-and-when/ (ICO 2017b). [Tieto haettu 1.1.2018].

ISO/IEC 27000 -sertifikaattiryhmä: https://www.iso.org/isoiec-27001-information-security.html [Tieto haettu 1.1.2018].

Kuchler, Hannah: Facebook flaw exposed monitors of terror groups. Financial Times, 16.6.2017. Saatavilla: https://www.ft.com/content/61bd61da-529b-11e7-bfb8-997009366969 (Kuchler 2017). [Tieto haettu 1.1.2018].

Tietosuojavaltuutetun toimisto: Laadi tietotilinpäätös. Tietosuojavaltuutetun opas. 24.4.2012. Saatavilla: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfpzNVCh/Laadi_tietotilinpaatos.pdf (TSV 2012). [Tieto haettu 1.1.2018].

Trafin julkaisuja 14/2017: Tietotilinpäätös 2015. Saatavilla: https://www.trafi.fi/filebank/a/1463394812/9478dbd63f9d555bc3cd6f5b5bc99e54/20667-Trafin_julkaisuja_14-2016_-_Tietotilinpaatos_2015.pdf (Trafi 2017). [Tieto haettu 1.1.2018].

Viestintävirasto: Viestintäviraston tietotilinpäätös 2016. Saatavilla: https://www.viestintavirasto.fi/attachments/Viestintaviraston_tietotilinpaatos_2016.pdf (Viestintävirasto 2017). [Tieto haettu 1.1.2018].

Väestörekisterikeskus: Väestörekisterikeskuksen tietotilinpäätös 2015 – tiivistelmä. 30.6.2016. Saatavilla: http://vrk.fi/documents/2252790/2783772/Tietotilinp%C3%A4%C3%A4t%C3%B6s_2015_tiivistelm%C3%A4/683bf75c-d416-475e-8824-96e99ebea966 (Väestörekisterikeskus 2016). [Tieto haettu 1.1.2018].

LYHENTEET

CNIL	Commission Nationale de l'Informatique et des Libertés, Ranskan tietosuojaviranomainen
EIS	Euroopan ihmisoikeussopimus
EIT	Euroopan ihmisoikeustuomioistuin
EU	Euroopan unioni
EUT	Euroopan unionin tuomioistuin
EUVL	Euroopan unionin virallinen lehti
EY	Euroopan yhteisö
HetiL	Henkilötietolaki (523/1999)
ICO	Information Commissioner's Office, Iso-Britannian tietosuojaviranomainen
KOM	Komission mietintö
OECD	The Organisation for Economic Co-operation and Development, Taloudellisen yhteistyön ja kehityksen järjestö
KP-sopimus	Kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus
SopS	Sopimussarja
Tietosuojasopimus	Euroopan neuvoston yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa käsittelyssä
TSV	Tietosuojavaltuutettu
WP29	Article 29 Working Party tietosuojatyöryhmä
YK	Yhdistyneet kansakunnat

TSV	Tietosuojavaltuutettu
WP29	Article 29 Working Party, artikla 29:n mukainen tietosuojatyöryhmä
YK	Yhdistyneet kansakunnat

1. Johdanto

Henkilötietojen suojan osalta EU:ssa ollaan uuden ajan kynnyksellä, kun pitkään valmisteltu EU:n yleinen tietosuoja-asetus[1] tulee sovellettavaksi toukokuussa 2018.

Henkilötietojen käsittely-ympäristö on muuttunut merkittävästi viime vuosikymmenien aikana. Henkilötietoja hyödynnetään yhä laajemmin ja eri toimijoiden toimesta, ja laskentatehon kasvaessa henkilötietoja käsitellään käyttötarkoituksiin, joita ei vielä muutama vuosikymmen sitten tunnettukaan. Myös henkilötietojen käsittelyn luonne on muuttunut merkittävästi: henkilötietoja ei enää kerätä virastoissa lomakkeilla, vaan tietoja kertyy arkipäivän toiminnoista. Sääntelyn ajantasaisuuden lisäksi tekninen kehitys asettaa haasteita myös viranomaisvalvonnalle, sillä tekniikan mahdollistama käsittelytoimien lisääntyminen ei enää mahdollista yksityiskohtaista, kaikkiin käsittelytoimiin kohdistuvaa kontrollia. Henkilötietojen käsittelyn toimintaympäristössä tapahtunut merkittävä muutos onkin aiheuttanut tarpeen uusille keinoille henkilötietojen suojan takaamiseksi.[2]

Tietosuoja-asetusta on kuvattu "mahdollisen taiteeksi": asetus on potentiaaliltaan merkittävä, mutta sen käytännön vaikutuksiin liittyy vielä epäselvyyksiä, eikä asetus määrittele yksityiskohtia mekanismeja, joilla potentiaali toteutettaisiin.[3]

Yksi merkittävimmistä tietosuoja-asetuksen tuomista uusista keinoista on osoitusvelvollisuus, eli rekisterinpitäjän velvollisuus pystyä osoittamaan käsittelytoiminnan vaatimustenmukaisuus. Osoitusvelvollisuus itsessään ei ole täysin uusi konsepti, vaan se esiintyi jo 80-luvulla OECD:n tietosuojasuosituksessa. Osoitusvelvollisuudella ei kuitenkaan ole ennen tietosuoja-asetusta ollut oikeudellisesti sitovaa merkitystä eurooppalaisessa tietosuojalainsäädännössä.

Osoitusvelvollisuus siirtääkin painopisteen tietosuojan vaatimustenmukaisuuden valvonnasta rekisterinpitäjille. Osoitusvelvollisuus on uudenlainen haaste rekisterinpitäjälle, ja se edellyttää huolellisempaa ja yksityiskohtaisempaa suunnittelua sekä käsittelytoimien hallintaa.

[1] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).
[2] WP 173, s. 3.
[3] Davies 2016 s. 291.

Toisaalta kun tutkimuksen kohteena on vasta sovellettavaksi tuleva asetus, liittyy tähän uuteen haasteeseen myös oikeustilan täsmentymättömyys: osoitusvelvollisuus on melko yleisluontoinen ja jopa tulkinnanvarainen vaatimus, eikä sen käytännön merkitys tai tarkka sisältö ole vielä täysin täsmentynyt. Tutkielmassa tarkastellaan osoitusvelvollisuuden muotoutumista tietosuojavaatimukseksi sekä osoitusvelvollisuuden rekisterinpitäjille asettamia keskeisiä vaatimuksia eli sitä, miten rekisterinpitäjät voivat osoittaa täyttäneensä osoitusvelvollisuuden asetuksen edellyttämällä tavalla.

1.1. Tutkimuskysymys ja tutkielman rakenne

Tutkielmassa perehdytään osoitusvelvollisuuteen EU:n tietosuoja-asetuksen keinona toteuttaa henkilötietojen suojaa. Tutkielmassa tarkastellaan ensiksikin osoitusvelvollisuuden muotoutumista tietosuojavaatimukseksi EU:n yleisessä tietosuoja-asetuksessa ja kontekstualisoidaan osoitusvelvollisuutta tietosuojauudistuksessa. Erityisesti käsitellään osoitusvelvollisuuden yhteyttä lainsäädäntöuudistuksen tavoitteisiin sekä taustaa sille, miksi osoitusvelvollisuus otettiin juuri nyt osaksi tietosuojalainsäädäntöä. Toiseksi tutkielmassa pyritään selvittämään, mitä osoitusvelvollisuudella tarkoitetaan, ja minkälaisia vuorovaikutussuhteita se luo, kiinnittäen huomiota etenkin osoitusvelvollisuuden sisältöön ja erityispiirteisin. Kolmanneksi tutkielmassa tarkastellaan osoitusvelvollisuuden laajuutta ja kohdistumista tietosuoja-asetuksessa sekä keskeisiä keinoja, joilla rekisterinpitäjä voi toteuttaa osoitusvelvollisuutta.

Kootusti tutkimuskysymykset ovat seuraavat:

1) Mitkä keskeiset seikat vaikuttivat osoitusvelvollisuuden muotoutumiseen EU:n tietosuoja-asetuksen tietosuojavaatimukseksi?
2) Mitä osoitusvelvollisuudella tarkoitetaan ja mikä sen keskeinen sisältö on?
3) Mitä keskeisiä vaatimuksia osoitusvelvollisuus asettaa rekisterinpitäjille EU:n tietosuoja-asetuksessa ja millä keinoin rekisterinpitäjä voi noudattaa vaatimusta?

Osoitusvelvollisuudella on luonteensa vuoksi kiinteä yhteys tietosuoja-asetuksen muihin velvoitteisiin eli siihen, mitä osoitusvelvollisuudella osoitetaan. Tutkielmassa ei ole tarkoitus kuitenkaan tyhjentävästi selvittää sitä, minkälaisia velvoitteita tietosuoja-asetuksesta seuraa rekisterinpitäjille tai sitä, miten asetusta noudatetaan, vaan tutkielmassa keskitytään

tarkastelemaan osoitusvelvollisuutta sekä siihen keskeisesti liittyviä dokumentointiin ja tietosuojahallintoon liittyviä velvoitteita.

Yhtenä asetuksen uusista velvoitteista osoitusvelvollisuus edellyttääkin rekisterinpitäjältä uudenlaista asennoitumista henkilötietojen käsittelyyn sekä rekisterinpitäjän oman toiminnan tarkastelua uusien vaatimusten valossa. Tutkielman alkuosassa käsitellään osoitusvelvollisuutta yleisellä tasolla, ja jäljempänä etenkin velvoitteen kohteena olevan rekisterinpitäjän kannalta. Tietosuoja-asetuksen on kuvattu olevan laadittu etenkin elinkeino- ja yritystoimintaa sääntéleväksi,[4] ja tutkielmassa tarkastellaankin osoitusvelvollisuutta juuri vaatimuksen kohteena olevan rekisterinpitäjän näkökulmasta, huomioiden elinkeinoelämälle tyypilliset tietohallintokäytännöt. Henkilötietojen käsittelijän vastuu ja rooli on rajattu tutkielman ulkopuolelle. Tutkielmassa ei myöskään käsitellä osoitusvelvollisuutta tuomioistuinmenettelyssä.

Tutkielman johdannon yhteydessä selvitetään keskeiset aihepiiriin liittyvät käsitteet. Tutkielman toisessa osassa käsitellään osoitusvelvollisuuden muodostumista tietosuojavelvoitteeksi EU:n yleisessä tietosuoja-asetuksessa. Aluksi tarkastellaan henkilötietojen suojaan liittyvää keskeistä lainsäädäntötaustaa. Tässä ei ole pyrkimyksenä antaa kattavaa kuvaa aiheesta, vaan lyhyesti johdattaa lainsäädännölliseen viitekehykseen taustaksi itse tutkimuskysymyksen tarkastelua varten. Tämän jälkeen toisessa osassa tarkastellaan osoitusvelvollisuutta etenkin keinona toteuttaa lainsäädäntöuudistuksen taustalla olevia tavoitteita, peilaten uudistuksessa esillä olleita tavoitteita osoitusvelvollisuuden sisältöön ja toiminnallisuuksiin.

Tutkielman kolmannessa osassa tarkastellaan osoitusvelvollisuuden luonnetta ja tasoja, pyrkien selvittämään, mitä osoitusvelvollisuudella tarkoitetaan. Lisäksi tarkastellaan velvollisuuteen liittyviä vuorovaikutussuhteita eli sitä, mille taholle osoitus kohdistuu. Tutkielman neljännessä osassa käsitellään osoitusvelvollisuutta tietosuoja-asetuksen velvoitteena. Tässä yhteydessä käsitellään osoitusvelvollisuutta tietosuoja-asetuksen periaatteiden sekä 24 artiklan yleisvelvoitteen kannalta, kiinnittäen huomiota siihen, mitä keskeisimpiä tekijöitä rekisterinpitäjän tulee osoittaa. Lisäksi osassa tarkastellaan keskeisimpiä toimenpiteitä ja käytäntöjä, joilla rekisterinpitäjä voi täyttää osoitusvelvollisuuden.

[4] Koillinen 2016, s. 585.

1.2. Metodi, tutkimusala ja keskeiset lähteet

Tutkimuksen kohteena on osoitusvelvollisuuden asema EU:n yleisessä tietosuoja-asetuksessa, ja tutkielmassa tarkastellaan velvoitteen muotoutumisen taustaa sekä sitä, miten osoitusvelvollisuudella suojataan henkilötietojen suojaa. Kysymyksiin pyritään vastaamaan lainopillisen tutkimuksen keinoin. Lainopillisessa tutkimuksessa tavoitteena on oikeusnormien tulkinta ja systematisointi.[5] Lainopillisessa systematisointityössä tutkitaan ja jäsennetään oikeudenalojen käsitteitä, oikeusperiaatteita sekä teoreettisia rakennelmia.[6] Tutkielmassa tarkastellaan EU:n tietosuojalainsäädäntöä etenkin tietosuoja-asetuksen, mutta myös kansallisen viitekehyksen osalta velvoitteiden kontekstualisoimiseksi. Tutkielmassa on siis myös oikeusvertailullisia elementtejä, joskaan tutkielman painopisteenä ei ole kansallisten sääntelyiden vertailu.

Tutkielma kohdistuu vasta tulevaisuudessa sovellettavaksi tulevaan lainsäädäntöön, kun tietosuoja-asetusta aletaan soveltaa noin puoli vuotta tutkielman laatimisen jälkeen. Haasteena tutkielmassa on asetuksen tarkastelun jääminen nyt *lex latan*, voimassaolevan oikeuden, ja *de lege ferendan*, eli sen, miten säännöstä tulisi tulevaisuudessa tulkita väliseen tilaan, kun asetuksen sisältö on tiedossa, mutta sitä ei vielä sovelleta, eikä siitä tästä johtuen ole myöskään olemassa vakiintunutta soveltamiskäytäntöä. Tutkielman näkökulman voidaankin katsoa olevan *lex lata* asetuksen sisällön ja *de lege ferenda* asetuksen soveltamisen osalta.

Henkilötietojen suoja ja tietosuoja asettuvat tyypillisesti viestintä- ja informaatio-oikeuden alalle. Oikeudenala tutkii etenkin informaation sääntelyä sekä sääntelyn tarvetta ja mahdollisuuksia.[7] Viestintä- ja informaatio-oikeus on oikeudenalana melko nuori, eikä se lukeudu täysin osaksi perinteisiä oikeudenaloja.[8] Viestintä- ja informaatio-oikeudelle onkin tyypillistä sen eteenpäin katsova luonne,[9] ja yhteiskunnan kehittyminen on tuonut uusia oikeudellisia ongelmia ja tutkintakysymyksiä viestintä- ja informaatio-oikeuden alalle, mukaan lukien uudet henkilötietojen suojaan liittyvät kysymykset.[10] Tietosuojaan liittyvät kysymykset sijoittuvatkin teknologian ja oikeuden leikkauspisteeseen, josta johtuen tutkielmassa tarkastellaan myös teknologian kehittymisen aiheuttamia tarpeita henkilötietojen suojan

[5] Hirvonen 2011, s. 22.
[6] Hirvonen 2011, s. 25.
[7] Korhonen 2006, s. 91.
[8] Korhonen 2006, s. 92.
[9] Saarenpää 2012 s. 430.
[10] Korpisaari 2015, s. 996.

sääntelylle sekä tutkitaan kehitystarpeiden ja -tavoitteiden heijastumista osoitusvelvollisuuden sisältöön. Koska tarkastelun kohteena on nimenomaan EU:n tietosuoja-asetus, tutkimusaihe sijoittuu informaatio- ja viestintäoikeuden ohella toisaalta myös EU-oikeudelliseen kontekstiin.

Tutkielmassa tarkastellaan osoitusvelvollisuutta nimenomaan EU:n uudistuvan tietosuojalainsäädännön yhteydessä, joten tietosuoja-asetus valmistelutöineen on yksi työn keskeisimmistä lähteistä. Lisäksi tutkielmassa käsitellään myös tietosuoja-asetusta edeltänyttä henkilötietodirektiiviä sekä siihen liittyvää oikeuskäytäntöä soveltuvin osin. Tietosuojauudistuksen ajankohtaisuudesta huolimatta tulee huomata, että henkilötietodirektiivillä sekä siihen liittyneellä oikeuskäytännöllä on merkittävä rooli eurooppalaisessa tietosuojasääntelyssä, ja merkittävä osa tietosuoja-asetuksen käsitteistä ja velvoitteista siirtyvät suoraan henkilötietodirektiivistä. Henkilötietojen suojan perusoikeusluonteen vuoksi tutkielmassa hyödynnetään myös tähän liittyvää aineistoa, joskaan tutkielman painopiste ei ole henkilötietojen suojan perusoikeuksiin liittyvissä kysymyksissä.

Tietosuojalainsäädännön lisäksi henkilötietodirektiivin 29 artiklan mukaisen tietosuojatyöryhmän[11] kannanotoilla on merkittävä rooli tarkastellessa henkilötietojen suojan ja osoitusvelvollisuuden kannalta keskeisiä seikkoja. Tietosuojatyöryhmä on neuvoa-antava elin, joka on antamissaan lausunnoissa ja suosituksissa selvittänyt etenkin henkilötietodirektiivin soveltamiseen ja tulkintaan liittyviä kysymyksiä sekä henkilötietojen suojan kannalta ajankohtaiseksi nousseita teemoja. Tutkielman aiheen kannalta erityisen olennaisia ovat osoitusvelvollisuutta käsitellyt, vuonna 2010 annettu mietintö, sekä tätä edeltänyt, yksityisyyden tulevaisuutta käsitellyt mietintö.[12] Huomattakoon kuitenkin, että nämä mietinnöt koskivat tietosuojauudistukseen mahdollisesti sisällytettävää osoitusvelvollisuutta, eli ne eivät varsinaisesti käsittele tietosuoja-asetuksen sanamuodon mukaista osoitusvelvollisuutta.

Koska asetuksen sanamuoto on verrattain avoin ja jättää osoitusvelvollisuuden konkreettiset toteuttamiskeinot avoimiksi, tutkielmassa selvitetään velvoitteen täyttämiseksi soveltuvia keinoja tarkastelemalla alan tyypillisiä käytäntöjä sekä viranomaisohjeita. Tarkentavia

[11] Tietosuojatyöryhmä (myös "*WP29"*) on henkilötietodirektiivin 29 artiklan perusteella perustettu riippumaton elin, jonka jäsenenä on jäsenmaiden tietosuojaviranomaisia sekä Euroopan tietosuojavaltuutettu. Ryhmä antaa ei-sitovia lausuntoja ja suosituksia. Kun tietosuoja-asetusta aletaan soveltaa toukokuussa 2018, Euroopan tietosuojaneuvosto tulee korvaamaan nykyisen tietosuojatyöryhmän.

[12] Opinion 3/2010 on the principle of accountability, WP 173, sekä The Future of Privacy, WP 168.

eurooppalaisia viranomaisohjeita ei tietosuoja-asetuksen mukaisesta osoitusvelvollisuudesta ole saatavilla, mutta tutkielmassa hyödynnetään laajasti edellä mainittua tietosuojatyöryhmän henkilötietodirektiivin aikaista, osoitusvelvollisuutta koskevaa aineistoa.

Tietosuoja-asetusta ei ole vielä sovellettu käytännössä, joten tutkielmaa varten ei ole ollut käytettävissä asetuksen soveltamiskäytäntöä. Tutkielman muita keskeisiä lähteitä ovat etenkin ulkomainen ja suomalainen oikeuskirjallisuus. Tietosuoja-asetuksen mukainen osoitusvelvollisuus on tätä kirjoitettaessa suhteellisen vähän käsitelty aihe, joten tältä kannalta oikeuskirjallisuutta on ollut käytettävissä suppeasti. Tästä johtuen tutkielmassa hyödynnetään myös tietosuoja-asetusta koskevia verkko- ja uutislähteitä, sekä tietosuoja-asetusta edeltänyttä, osoitusvelvollisuutta yleisellä tasolla käsitellyttä oikeuskirjallisuutta. Tutkielman painopiste ei ole suomalaisen tietosuojalainsäädännön tarkastelussa, joskin sitä käsitellään soveltuvin osin toimintaympäristön ja kontekstin havainnollistamiseksi.

1.3. Keskeisiä määritelmiä

Tietosuojalla tarkoitetaan *henkilötietojen suojan* oikeudellista sääntelyä. Käsitteestä huolimatta tietosuojalla pyritään suojaamaan luonnollisia henkilöitä ja heidän oikeuksiaan, eikä sinänsä tietoa itsessään.[13] Tietosuoja määrittelee lainsäädännön keinoin toteutettavat rajat ja edellytykset henkilötietojen sallitulle käsittelylle.[14]

Henkilötiedon käsite on henkilötietojen suojan ytimessä, ja määrittelyllä onkin oleellinen rooli tietosuojalainsäädännön soveltamisalan laajuuden tarkastelussa.[15] Tietosuoja-asetuksen 4 artiklan 1-kohdan mukaan henkilötietoina pidetään kaikkia sellaisia tietoja, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön. Tunnistettavuus voi toteutua joko suoraan tai epäsuorasti tunnistetietojen tai henkilölle tunnusomaisen tekijän perusteella,

[13] Saarenpää 2012, s. 319. Sama käsitteellinen kohdistuminen esiintyy muissa kielissä, kuten saksassa (*Datenschutz*) tai englannissa (*data protection*), joskin angloamerikkalaisessa yhteydessä käytetään myös termiä *data privacy*.

[14] De Hert — Gutwirth 2009, s. 4.

[15] WP 136 s. 3. Tietojen tulee siis olla juuri henkilötietoja, jotta ne tulevat henkilötietojen suojan piiriin. Todettakoon, että henkilötietolainsäädäntö lähtee tarkkarajaisesta määrittelystä, jossa tiedot joko ovat tai eivät ole henkilötietoja, eikä näille ole varsinaista välimuotoa. Tiettyjä kriittisiä tietoja, kuten arkaluonteisia tietoja, suojataan kuitenkin erikseen. Lisäksi asetukseen on tuotu termi pseudonymisoitu henkilötieto. Kyse ei kuitenkaan ole varsinaisesti erillisestä henkilötietoluokasta, vaan tiedosta, josta on poistettu suora tunnistettavuus. Pseudunonymisoidutkin tiedot ovat siis henkilötietoja. Tästä laajemmin tietosuoja-asetuksen 26 artikla, ks. myös asetukesn 4(5) artikla.

kuten fyysisestä, fysiologisesta, geneettisestä, psyykkisestä, taloudellisesta, kulttuurisesta tai sosiaalisesta tekijästä.[16]

Määritelmä vastaa pitkälti henkilötietodirektiivin mukaista henkilötiedon määritelmää. Jo henkilötietodirektiivin mukaisessa määritelmässä on katsottu kuvastuvan kautta lainsäädäntöprosessin ilmenevä lainsäätäjän pyrkimys henkilötiedon laajaan määritelmään.[17] Henkilötietojen määritelmä ei ole staattinen, vaan käsite elää teknologian kehittyessä, kun kerättävien tietojen kenttä laajenee ja tietoja pystytään yhdistämään yhä kattavammilla tavoilla luonnollisiin henkilöihin uusien teknologioiden myötä sekä laskentatehon kehittyessä.[18]

Rekisteröidyllä tarkoitetaan luonnollista henkilöä, joka on tunnistettu tai tunnistettavissa häneen liittyvistä tiedoista. Yhteys luonnolliseen henkilöön on ainakin silloin, kun tiedot kertovat hänestä[19] tai kun henkilö esiintyy tiedoissa.[20] Lisäksi tietojen on katsottu koskevan henkilöä, jos tieto *"liittyy hänen identiteettiinsä, luonteenpiirteisiinsä tai käyttäytymiseensä, tai jos tällaista tietoa käytetään sen ratkaisemiseksi, miten kyseistä henkilöä kohdellaan tai arvioidaan"*.[21] Tällöin myös ensisijaisesti esimerkiksi tavaroita, prosesseja tai tapahtumia koskevat tiedot saattavat joissain tilanteissa koskea epäsuorasti myös henkilöä, jolloin kyse on henkilötiedoista.[22]

Rekisterinpitäjällä tarkoitetaan tietosuoja-asetuksessa *"luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa*

[16] Asetuksessa sanamuotoa on laajennettu tunnistetietojen osalta, joista on esimerkinomaisesti mainittu sijaintitiedot sekä verkkotunnistetiedot. Lisäksi maininta geneettisistä tekijöistä on lisätty asetuksen määritelmään.

[17] WP 136, s. 4. Henkilötiedon määritelmä on ajan saatossa laajentunut. Esimerkiksi jo kumotussa Suomen henkilörekisterilaissa (471/1987) henkilötiedon määritelmästä oli rajattu pois tiedot, jotka liittyvät luonnolliseen henkilöön muussa ominaisuudessa kuin yksityishenkilönä, esimerkiksi ammatinharjoittamista tai julkista tehtävää koskevat tiedot. Kun henkilörekisterilaki korvattiin henkilötietolailla (22.4.1999/523), laajennettiin henkilötiedon käsitettä henkilötietodirektiivin käsitteen mukaiseksi.

[18] Tietoja saatetaan pystyä myöhemmin yhdistämään luonnolliseen henkilöön esimerkiksi hyödyntämällä teknologiaa, jota ei tiedon keräyshetkellä ollut käytettävissä tai vielä edes keksitty. Tästä esimerkkinä useat tunnetut tapaukset, joissa anonymisoitua tietoa - joka ei siis jo määritelmänsäkään mukaan ole henkilötietoa - on kyetty useissa tapauksissa yhdistämään takaisin luonnolliseen henkilöön yhdistämällä anonymisoitua tietoa muiden tietokantojen tietoihin. OECD 2013, s. 97. Anonymisointiin liittyvistä haasteista tarkemmin WP 216. Koska anonymisoitu data on anonyymia vain, jos tunnistettavuutta ei voida palauttaa, saattaa deidentifikaatioteknologian kehittyminen koetella jatkossa anonyymin tiedon ja tätä kautta myös henkilötiedon käsitteen rajoja.

[19] WP 136, s. 9-10.

[20] Esimerkiksi videotallenne, jolla henkilö esiintyy, on katsottu henkilötiedoksi. C-212/13 Rynes, kohta 22.

[21] WP 105, s. 8.

[22] WP 136, s. 9. Esimerkiksi mobiililaitteen IMEI-tunniste viittaa sinänsä laitteeseen, mutta käytännössä sillä voidaan tyypillisesti tunnistaa uniikit käyttäjät eli tieto yhdistyy laitetta käyttävään luonnolliseen henkilöön. Tästä myös WP 202 s. 8.

määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot". Rekisterinpitäjän käsite on luonteeltaan toiminnallinen, eli sen tarkoituksena on kohdistaa vastuu tahoon, joka tosiasiallisesti määrittelee käsittelytoimet.[23] Oleellista on etenkin käsittelyn tarkoitusten määritteleminen: joissakin tilanteissa henkilötietojen käsittelyyn liittyvät tekniset ja organisatoriset keinot saattavat jäädä käsittelijän tai muun tahon määriteltäväksi.[24] Tutkielmassa rekisterinpitäjän käsite on erittäin oleellisessa asemassa, koska sillä on keskeinen merkitys osoitusvelvollisuuden kohdistumisen kannalta — juuri rekisterinpitäjä on se taho, jonka vastuulla osoitusvelvollisuuden noudattaminen on. Myös tietosuojatyöryhmä on korostanut, että rekisterinpitäjän käsitteen määrittelyssä on kyse ensisijaisesti vastuun jakamisesta: rekisterinpitäjän käsite määrittää tahon, joka vastaa tietosuojalainsäädännön noudattamisesta.[25]

Henkilötietojen käsittely viittaa henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin kohdistettavaan toimintaan. Asetuksessa henkilötietojen käsittelyllä tarkoitetaan kaikkia henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin kohdistettavia toimenpiteitä.[26] Myös henkilötietojen käsittelyn tulkinta on laaja, ja asetuksessa mainitaankin esimerkinomaisesti laaja joukko toimenpiteitä: tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen tai muuttaminen, haku, kysely, käyttö, luovuttaminen siirtämällä, levittämällä tai asettamalla muutoin saataville, tietojen yhteensovittaminen tai yhdistäminen, rajoittaminen, poistaminen ja tuhoaminen ovat kaikki käsittelyä. Niin sanottu kotitalouspoikkeus rajaa luonnollisten henkilöiden pienimuotoisen, arkielämän piiriin kuuluvan henkilötietojen käsittelyn tietosuojalainsäädännön soveltamisalan ulkopuolelle.[27]

---

[23] WP 169, s. 8-9.

[24] WP 169, s. 13. Etenkin teknisesti haastavien tai monimutkaisten käsittelyiden osalta käsittelijällä saattaa olla paremmat edellytykset valita käsittelyyn soveltuvat tekniset ja organisatoriset keinot.

[25] WP 169, s. 4. Tämä ei kuitenkaan tarkoita, että käsittelijä vapautuisi täysin käsittelyyn liittyvästä vastuusta, ks. käsittelijän vastuusta tarkemmin 28 artikla ja rekisteröidyn oikeudesta saada korvaus kärsimistään vahingoista 82 artikla.

[26] Tietosuoja-asetuksen 4(1) artikla.

[27] Kotitalouspoikkeus ei sinänsä tarkoita, etteikö tietosuojalainsäädäntö koskisi mitään luonnollisten henkilöiden suorittamaa henkilötietojen käsittelyä, vaan poikkeus koskee "yksinomaan henkilökohtaisessa tai kotitaloutta koskevassa toiminnassa" tehtyä käsittelyä. Huomiota kiinnitetään erityisesti käsittelyn laatuun, luonteeseen ja mittakaavaan, ja luonnollisen henkilön voidaan katsoa olevan rekisterinpitäjä, jos toiminta ylittää kotitalouspoikkeuksen rajat. Näin esim. uskonnolliseen vapaaehtoistyöhön liittynyt C-101/01 Lindqvist, kohdat 45 ja 48, ja kotipihaan osoitettua mutta myös julkista paikkaa kuvannutta valvontakameraa koskenut C-212/13 Rynes, kohta 33. Kotitalouspoikkeus koskee kuitenkin nimenomaisesti vain luonnollista henkilöä, tästä myös C-73/07 Satamedia, kohta 44.

Kuten aiemmin mainittiin, *henkilötietojen käsittelijän* rooli ja vastuut sekä rekisterinpitäjän ja henkilötietojen käsittelijän välinen suhde on rajattu tutkielman ulkopuolelle. Käsittelijän määrittely on kuitenkin oleellista rekisterinpitäjyyden rajojen ja vastuun kohdistumisen tunnistamiseksi.[28] Tietosuoja-asetuksessa henkilötietojen käsittelijällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.[29] Käsittelijä on rekisterinpitäjästä erillään oleva taho, jonka käyttö perustuu rekisterinpitäjän päätökseen.[30] Käsittelijän suorittaman tietojen käsittelyn laajuus ja luonne voivat vaihdella. Käsittelijän asema määritellään käsittelytoimikohtaisesti, eli sama taho voi toimia toisessa käsittelytoimessa rekisterinpitäjänä ja toisessa käsittelytoimessa henkilötietojen käsittelijänä, joten käsittelijän aseman määrittelyssä tuleekin huomioida käsittelytoimikohtaiset tieto- ja toimintakokonaisuudet eli se, minkä luonteista käsittelyä käsittelijä suorittaa, ja mikä on käsittelyn varsinainen tarkoitus.[31] Käsittelijän asema ei siis perustu toimijan luonteeseen, vaan käsittelytoimeen liittyviin konkreettisiin toimiin.[32]

[28] Rekisterinpitäjän ja tietojen käsittelijän roolin määrittely voi muodostua tapauskohtaisesti hyvinkin merkittäväksi juuri vastuun jakamisen kannalta. Määrittely ei ole aina yksinkertaista tai itsestäänselvää. Esimerkiksi Google Spain -tapauksessa julkisasiamies katsoi internethakukoneen palveluntarjoajan toimivan käsittelijän roolissa hakukoneen välimuistissa olevien sisältöjen osalta. (Ratkaisuehdotus asiassa C-131/12 Google Spain, kohdat 91 ja 100). EUT päätyi katsomaan hakukonetoimintaa harjoitettavan tässä yhteydessä rekisterinpitäjän roolissa (C-131/12 Google Spain, kohta 41). EUT myös korosti, että rekisterinpitäjän laajan määritelmän taustalla on tavoite varmistaa rekisteröityjen tehokas ja kattava suojelu (Google Spain, kohta 34). Roolien selkeän jaon merkityksestä myös tietosuoja-asetuksen 79 resitaali.

[29] Tietosuoja-asetuksen 4(8) artikla.

[30] WP 169, s. 24.

[31] WP 169, s. 24. Esimerkiksi ulkoistettuja palkkahallinnon palveluja tarjoava yritys voi toimia käsittelemiensä asiakasyritysten palkkatietojen osalta henkilötietojen käsittelijänä, ja omien työntekijöidensä tietojen sekä asiakkuuksiensa hallintaan (esimerkiksi tiedot asiakasyritysten kontaktihenkilöistä) liittyvien tietojen osalta rekisterinpitäjänä.

[32] WP 169, s. 32. Todettakoon myös, että tietosuoja-asetuksen mukaan henkilötietojen käsittelijä saattaa muuttua rekisterinpitäjäksi, jos tämä asetuksen vastaisesti määrittelee käsittelyn tarkoitukset ja keinot eli ottaa roolin, joka tosiasiallisesti kuuluisi rekisterinpitäjälle (tietosuoja-asetuksen 26(10) art.).

2. Osoitusvelvollisuuden muodostuminen yleiseksi tietosuojavaatimukseksi

2.1. Henkilötietojen suojan lainsäädännöllinen viitekehys

2.1.1. Yksityisyyden suoja ja henkilötietojen suoja perusoikeutena

Henkilötietojen suojalla on kiinteä yhteys yksityisyyden suojaan, ja näitä molempia suojataan perusoikeuksien tasolla. Henkilötietojen suojan ja yksityisyyden suojan välinen suhde on jokseenkin vaikeasti määriteltävissä ja rajattavissa.[33] Henkilötietojen suoja kattaa myös sellaiset henkilötiedot, jotka eivät välttämättä kuulu yksityiselämän alaan. Tällaisia tietoja ovat esimerkiksi julkisena pidettävät tiedot, kuten tieto henkilön työpaikasta tai vaikkapa sormenjälkitieto.[34] Toisaalta yksityiselämän suoja kattaa myös muita ulottuvuuksia kuin henkilötietojen suojan, kuten esimerkiksi kodin ja perhe-elämän suojan.[35] Henkilötietojen suojan ja yksityisyyden suojan voidaan siis katsoa olevan limittäisiä oikeuksia.

Henkilötietojen suoja sekä yksityisyyden suoja on systematisoitu lainsäädäntöinstrumenteissa hieman toisistaan poiketen. Euroopan ihmisoikeussopimuksessa henkilötiedot saavat suojaa yksityisyyden suojan kautta. EIS 8(1) artikla suojaa yksityis- ja perhe-elämää, eikä siinä nimenomaisesti mainita henkilötietojen suojaa. Henkilötietojen suojan on EIT:n oikeuskäytännössä katsottu kuuluvan osaksi 8. artiklan soveltamisalaa.[36] Vastaavasti YK:n KP-sopimuksessa (17 artikla) suojataan vain yksityisyyden suojaa yleisellä tasolla.

Henkilötietojen suojan osalta perusoikeuksien horisontaalivaikutuksen, eli niiden vaikutuksen yksityisten tahojen välisessä suhteessa korostuu — henkilötietojen suoja on toki keskeistä julkisen vallan ja yksilön välisessä vertikaalisuhteessakin, mutta henkilötietojen käsittely-ympäristössä merkittävä osa henkilötietojen käsittelystä tapahtuu yksityisten toimijoiden toimesta. EIT:n osalta horisontaalinen vaikutus tulee keskeisesti esille lainsäätäjän positiivisen velvoitteen kautta: EIT:n oikeuskäytännössä perusoikeusvelvoitteiden on katsottu luovan myös positiivisia velvollisuuksia lainsäätäjälle, jonka on huolehdittava siitä, että lainsäädäntö sekä

[33] Ks. esim. Koillinen 2013, s. 171; Lindroos-Hovinheimo 2016, s. 122-123.
[34] Lindroos-Hovinheimo 2016, s. 134.
[35] Pitkänen - Tiilikka - Warma 2014, s. 15. Tästä myös Koillinen 2013, s. 180. Toisaalta perinteisesti yksityiselämän suojan piiriin kuuluviin osa-alueisiin, kuten kodin suojaan, voi teknologian kehittyessä yhdistyä henkilötietojen suojaan liittyviä uusia kysymyksiä esimerkiksi IoT-tekniikan myötä.
[36] Leander v. Ruotsi, kohta 48. Esimerkiksi tapauksessa S. and Marper v. Yhdistyneet Kuningaskunnat katsottiin jo yksityiselämää koskevan tiedon keräämisen johtavan mahdollisesti 8 artiklan loukkaamiseen. Tästä Koillinen s. 2013, s. 177 .

oikeuskäytäntö ylläpitävät perusoikeuksien turvaa ja turvaavat riittävät, käytännölliset ja tehokkaat takeet perusoikeuksien toteutumiseksi.[37] Yksityisten tekemät perusoikeusrikkomukset voivat tällöin johtaa valtion vastuuseen silloin, kun positiivista velvoitetta ei ole riittävästi noudatettu.[38]

Tätä velvoitetta havainnollistaa EIT:n tapaus I v. Suomi, eli ns. urkintatapaus, jossa oli kyse sairaalan toimenpiteistä potilastietojen suojaamiseksi. Tapauksessa katsottiin, että valtio ei ollut toteuttanut positiivista velvollisuutta henkilön yksityisyyden suojan, tässä tapauksessa potilastietojen suojaamiseksi: tämän suojan katsottiin ulottuvan yksilöiden väliseen toimintaan.[39] Perusoikeuksien tosiasiallisen toteutumisen siis on katsottu vaativan rekisterinpitäjiltä riittäviä menettelyjä henkilötietojen suojaan liittyvien periaatteiden toteuttamisesta käytännössä.[40]

Ratkaisusta käy ilmi, että Euroopan ihmisoikeussopimuksen vaikutukset koskevat yksityisten henkilöiden ja viranomaisten välisen suhteen lisäksi valtion velvollisuutta ryhtyä toimenpiteisiin sopimuksessa suojattujen perusoikeuksien turvaamiseksi myös yksityishenkilöiden välisissä suhteissa.[41] Henkilötietojen suojan perusoikeusluonteen vuoksi lainsäädännön tuleekin olla riittävää ja toimivaa perusoikeussuojan takaamiseksi. Tekninen kehitys ja henkilötietojen suojaan kohdistuvien uhkien ennakoimattomuus saattaakin osoittautua haasteeksi lainsäätäjälle tämän pyrkiessä löytämään tehokkaita suojakeinoja, jotka takaavat henkilötietojen suojan toteutumisen myös esimerkiksi teknologisten muutosten yhteydessä.

EIT:n ratkaisukäytäntö on ollut keskeisessä asemassa myös EU:n perusoikeusjärjestelmän kehitykselle.[42] Toisin kuin EIS:ssa, EU:n perusoikeuskirjassa henkilötietojen suoja on kuitenkin yksityiselämän suojaan nähden itsenäinen oikeus. Lissabonin sopimuksen myötä perusoikeuskirjasta tuli oikeudellisesti sitova. Perusoikeuskirjan 7 artiklassa säädetään yksityisyyden suojasta, ja perusoikeuskirjan 8 artiklassa säädetään henkilötietojen suojasta. EUT:n oikeuskäytännössä on korostettu oikeuksien itsenäisyyttä.[43] Henkilötietojen suojaa on

[37] Pitkänen — Tiilikka — Warma 2014 s. 19.
[38] De Hert 2011, s. 95.
[39] Tzanou 2017, s. 47.
[40] De Hert 2012, s. 202.
[41] Pitkänen — Tiilikka — Warma 2014, s. 11.
[42] González-Fuster 2014, s. 170.
[43] Tästä Client Earth C-615/13, kohta 32: ”[henkilötietojen suojaa yhteisöjen toimielinten toiminnassa koskevan asetuksen 45/2001] henkilötietojen käsite ei vastaa yksityiselämää koskevien tietojen käsitettä”.

punnittu EUT:n oikeuskäytännössä toisten perusoikeuksien kanssa, ja etenkin henkilötietojen suojan suhde omistusoikeuteen[44] sekä sananvapauteen[45] on ollut toistuvasti esillä EUT:n ratkaisukäytännössä.

Henkilötietojen suojan perusoikeutta korostetaan myös heti tietosuoja-asetuksen ensimmäisessä resitaalissa. Toisaalta tulee huomata, ettei kyse ole absoluuttisesta oikeudesta.[46] Asetuksella tavoitellaankin henkilötietojen suojan lisäksi myös henkilötietojen vapaata liikkuvuutta. Henkilötietojen suojaa tuleekin tarkastella suhteessa muihin perusoikeuksiin. Tavoitteiden yhteensovittamisen tarve sekä henkilötietojen suojan keskeinen tarkoitus ilmenekin tietosuoja-asetuksen alun resitaalista: *"Henkilötietojen käsittely olisi suunniteltava niin, että se palvelee ihmistä."*[47]

2.1.2. Tietosuojasääntelyn kansainvälinen kehitys

Henkilötietojen suoja on noussut ajankohtaiseksi sääntelyn kohteeksi viimeisen 50 vuoden aikana, ja etenkin Euroopan unionia on kuvailtu edelläkävijäksi tietosuojalainsäädännön alalla.[48] Euroopan yhteisössä havahduttiin 70-luvulla tietokoneiden sekä sähköisen tietojenkäsittelyn yleistymiseen sekä tarpeeseen laatia lainsäädännöllinen kehys teollisen tietojenkäsittelyn tueksi. Tuolloin kiinnitettiin huomiota etenkin yhtenäisen sääntelyn tarpeeseen sekä perusoikeudelliseen suojaan siitä huolimatta, ettei yhdessäkään eurooppalaisessa valtiossa vielä tuolloin tunnettu henkilötietojen suojaa perusoikeutena.[49]

Alustava työ henkilötietojen suojaa koskevan sääntelyn kehittämiseksi alkoi 70-luvulla, jolloin yhteisöjen komissio perusti muun muassa henkilötietojen käsittelyä tarkastelevan työryhmän,[50]

---

[44] Omistusoikeuteen liittyvät kysymykset ovat koskeneet etenkin tekijänoikeussuojaa ja henkilötietojen suojan laajuutta tekijänoikeusloukkaustapauksissa. Tästä mm. C-275/06 Promusicae, C-360/10 Netlog ja C-416/10 Bonnier Audio.

[45] Mainittakoon varhainen henkilötietojen suojaa perusoikeutena koskenut C-101/01 Lindqvist, jossa arvioitiin henkilötietojen julkaisemista verkkosivuilla, verotietojen julkaisemisen arviointia journalistisena tulkintana koskenut C-73/07 Satamedia, sekä hakukoneen tuloksia koskenut C-131/12 Google Spain. Google Spain -tapauksessa sivuttiin myös omistusoikeutta: henkilötietojen suojaan puuttumista arvioitaessa katsottiin tietoa hakevien tiedonintressin olevan perusteltua ottaa mukaan puuttumisen arviointiin, kun taas pelkästään hakukoneen taloudellisen intressin huomioimisen ei katsottu olevan perusteltua. (em. tapaus, kohta 81).

[46] Tämä todetaan myös tietosuoja-asetuksen neljännessä resitaalissa: *"Oikeus henkilötietojen suojaan ei ole absoluuttinen; sitä on tarkasteltava suhteessa sen tehtävään yhteiskunnassa ja sen on suhteellisuusperiaatteen mukaisesti oltava oikeassa suhteessa muihin perusoikeuksiin."*

[47] Tietosuoja-asetuksen 4 resitaali.

[48] Mouzakiti 2015, s. 39.

[49] González-Fuster 2014, s.122.

[50] Working Party on Data Processing and Protection of Liberties.

joskin tuolloin työ jäi kuitenkin vielä tutkimus- ja mietintötasolle.[51] Merkittäviä askeleita kohti tietosuojalainsäädäntöä otettiin 80-luvun alussa, jolloin laadittiin sekä Euroopan neuvoston tietosuojayleissopimus ja OECD:n tietosuojasuositus.

Osoitusvelvollisuus esiintyi ensimmäisen kerran erillisenä tietosuojaan liittyvänä periaatteena OECD:n vuonna 1980 hyväksymässä tietosuojasuosituksessa.[52] OECD:n tietosuojasuositus on valtioille suunnattu lainsäädäntösuositus,[53] ja se koostuu yleisperiaatteista, joista osoitusvelvollisuus ilmaistaan kohdassa 14 seuraavasti: *"A data controller should be accountable for complying with measures which give effect to the principles stated above"*.

Osoitusvelvollisuutta itsessään ei määritellä OECD:n tietosuojasuosituksessa. Oikeuskirjallisuudessa sen merkityksen on katsottu olevan luonteeltaan lähellä "vastuuta".[54] Suosituksessa osoitusvelvollisuuden tarkoituksena on sekä kohdistaa vastuu tietosuojaperiaatteiden noudattamisesta rekisterinpitäjälle, että varmistaa kaikkien suosituksessa määriteltyjen periaatteiden tulevan noudatetuksi käytännössä.[55] OECD:n suositus on suunnattu jäsenvaltioille, joten säännöksen tavoitteena onkin kannustaa jäsenvaltioita rakentamaan mekanismeja, joilla taataan rekisterinpitäjän vastuun toteutuminen.[56]

Toinen 80-luvun olennaisista säännöksistä tietosuojan alalla on vuonna 1981 hyväksytty Euroopan neuvoston yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä eli ns. tietosuojayleissopimus.[57] Sopimus velvoittaa sen osapuolia, eli sopijavaltioita. Kaikki EU:n jäsenvaltiot ovat ratifioineet yleissopimuksen. Suomessa sopimus tuli voimaan vuonna 1992.[58]

Tietosuojayleissopimus oli ensimmäinen tietosuojaa koskeva oikeudellisesti sitova kansainvälinen sopimus ja siten huomattava askel henkilötietojen itsenäisen lainsäädännöllisen suojan muodostumisessa. Tietosuojayleissopimuksella tuotiin tietosuoja eli *"data protection"*

[51] González-Fuster 2014, s. 117.
[52] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
[53] Korhonen 2003, s. 93.
[54] Englanniksi "responsibility" sekä "liability", Raab 2012, s. 16.
[55] Alhadeff — Van Alsenoy — Dumortier 2012, s. 7.
[56] Alhadeff — Van Alsenoy — Dumortier 2012, s. 7. OECD:n suositukset päivitettiin 2013 vastaamaan teknologisen kehityksen sekä henkilötietojen merkityksen korostumisen aiheuttamiin tarpeisiin, tästä tarkemmin kohdassa 4.3.2.
[57] Tietosuojayleissopimus, ETS nro 108.
[58] SopS 35/1992.

terminä ensimmäistä kertaa oikeudellisesti sitovaan, kansainväliseen sopimukseen. Lisäksi yleissopimus yhdisti henkilötietojen suojan perusoikeuksien ja -vapauksien turvaamiseen, korostaen sen merkitystä näiden oikeuksien turvaamisessa. Tietosuojayleissopimuksella tuotiin myös esiin yhteys henkilötietojen suojan sekä EIS:n 8 artiklan mukaisen yksityisyyden suojan välillä.[59]

Tietosuojayleissopimus sekä OECD:n tietosuojasuositus valmisteltiin yhteistyössä ja samanaikaisesti, ja niiden yleisperiaatteet ovat sisällöltään lähellä toisiaan.[60] OECD:n tietosuojasopimuksesta poiketen osoitusvelvollisuuteen ei kuitenkaan viitata tietosuojayleissopimuksessa.

Direktiivi yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, eli henkilötietodirektiivi,[61] annettiin lokakuussa 1995. Tietosuojayleissopimuksella sekä OECD:n periaatteilla oli myös merkittävä rooli henkilötietodirektiivin laatimisessa, ja direktiivillä pyrittiinkin täsmentämään tietosuojayleissopimuksen periaatteita.[62]

Henkilötietodirektiivillä oli kaksoistavoite tietosuojalainsäädännön yhdenmukaistamiselle: direktiivillä haluttiin sekä vahvistaa henkilötietojen suojaa, että edistää sisämarkkinoiden toimintaa. Tietosuojalla ja sisämarkkinoilla onkin vahva yhteys, ja henkilötietodirektiivi annettiin sisämarkkinatoimivallan perusteella.[63] Kuten tietosuoja-asetusta tällä vuosikymmenellä, myös henkilötietodirektiivin tarvetta perusteltiin teknologisen kehityksen tuomilla haasteilla.[64]

---

[59] González-Fuster 2014, s. 88-89.

[60] Korhonen 2003, s. 93 ja HE 96/1998 vp, s. 13. OECD-yhteistyöstä laajemmin González-Fuster 2014, s. 87. Oleellisena erona tietosuojayleissopimuksen sekä OECD:n yleissopimuksen välillä mainittakoon ero tavoitteissa: OECD:n yleissopimuksen kaksoistavoite oli yksityisyyden suojan toteutuminen ja tietojen vapaa kulku, kun taas tietosuojayleissopimuksen yksinomaisena tarkoituksena oli henkilötietojen suojan vahvistaminen. González-Fuster 2014, s. 89.

[61] Euroopan parlamentin ja neuvoston direktiivi 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, usein myös *tietosuojadirektiivi*.

[62] HE 96/1998 vp s. 15. Tietosuojasopimuksen sekä OECD:n periaatteiden merkityksestä myös Korhonen 2003, s. 94.

[63] Tietosuojalainsäädännön yhtenäistäminen on ollut yksi sisämarkkinoiden kehittämisen keino: pyrkimyksenä on ollut estää yksityisyyden suojan käyttäminen esteenä henkilötietojen liikkumiselle jäsenvaltioiden välillä. Wallin 2001, s. 353-534.

[64] Van Hoecke — Dhont 1999, s. 130. Ensimmäiset eurooppalaiset tietosuojaa koskevat lait olivat 70-luvulta, aikaisimpana Ruotsin Datalagen vuodelta 1973. Datalagenista laajemmin Bennett 1992, s. 63. Toisaalta osassa EU-maista ei ollut henkilötietojen suojaa koskevaa lainsäädäntöä ennen henkilötietodirektiivin implementointia, Van Hoecke — Dhont 1999, s. 112.

Suomessa tietosuojalainsäädännön tarvetta tarkasteltiin jo 70-luvun alussa, mutta hanke raukesi erimielisyyksiin.[65] Myöhemmin 80-luvulla valmisteltu henkilörekisterilaki tuli voimaan vuoden 1988 alussa, ja sen valmistelussa hyödynnettiin vuoden 1981 tietosuojayleissopimusta.[66] Henkilörekisterilaki ehti olla voimassa noin kymmenen vuotta.

Henkilörekisterilain korvasi henkilötietodirektiiviin perustunut henkilötietolaki, joka tuli voimaan vuonna 1999. Henkilötietolakia säädettäessä henkilörekisterilainsäädännön katsottiin kaipaavan ajanmukaistamista ja selkeyttämistä yhteiskunnallisesta ja teknisestä kehityksestä johtuen, ja myös aiemmassa lainsäädäntötyössä 1990-luvulla oli tunnistettu henkilörekisterilainsäädännön kokonaistarkistuksen tarve.[67] Henkilötietolakia koskeneessa hallituksen esityksessä todettiin, että sen lisäksi, että henkilötietojen käsittelyn tekniikat ovat kehittyneet nopealla tahdilla henkilörekisterilain voimassaoloaikana, tulee tällainen kehittyminen jatkumaan tulevaisuudessakin. Lainsäätäjä tunnistikin tarpeen tehdä lainsäädännöstä "tulevaisuudenpitävää". Tässä yhteydessä todettiin myös pyrkimys teknologianeutraaliin sääntelyyn niin, ettei sanamuoto sitoisi sääntelyä tietynlaiseen tekniikkaan.[68]

Henkilötietodirektiivin implementoinnissa jäsenvaltiot ovat päätyneet toisistaan poikkeaviin lainsäädäntöratkaisuihin.[69] Suomessa henkilötietolainsäädäntö on joiltain osin kattavampaa kuin henkilötietodirektiivin vähimmäisvaatimukset,[70] toisaalta esimerkiksi rekisterinpitäjän ilmoitusvelvollisuus valvontaviranomaisille on suppeampi kuin useassa muussa jäsenvaltiossa. Eroavaisuuksien direktiivin kansallisessa täytäntöönpanossa jäsenmaiden välillä voidaan katsoa vaikeuttaneen direktiivin sisämarkkinatavoitteen toteutumista käytännössä.[71]

Henkilötietolaki on henkilötietojen suojaa koskeva yleislaki, ja lisäksi tietosuojasta säännellään useilla erityislaeilla.[72] Toimialakohtainen erityissääntely on tarpeen johtuen etenkin

[65] Saarenpää 2012, s. 328.
[66] Saarenpää 2012, s. 328.
[67] Tästä HE 96/1998 vp.
[68] HE 96/1998 s. 23.
[69] Saarenpää 2012, s. 329.
[70] Saarenpää 2012, s. 329.
[71] KOM (2010) 609, s. 10.
[72] Erityislainsäädännöstä mainittakoon erityisrekistereihin liittyvät lait (mm. väestötietolaki, laki arvo-osuusjärjestelmästä), viranomaisten tehtäviin ja toimintoihin liittyvät lait, joissa säädetään myös henkilötietojen käsittelyyn liittyvistä seikoista (mm. laki potilaan asemasta ja oikeudesta, laki sosiaalihuollon asiakkaan asemasta ja oikeuksista, laki verotustietojen julkisuudesta ja salassapidosta) sekä yksityisen sektorin toimijoita koskevat alakohtaiset lait (esim. laki luottolaitostoiminnasta).

perustuslain 10.1§:n mukaisesta velvoitteesta säätää henkilötietojen suojasta lailla.[73] Henkilörekisterilaissa, henkilötietodirektiivissä eikä siihen perustuneessa henkilötietolaissa ollut nimenomaista säännöstä osoitusvelvollisuudesta.

2.2. Henkilötietodirektiivistä yleiseen tietosuoja-asetukseen

Tietosuojauudistusta alettiin valmistella jo vuonna 2009, ja EU:n yleinen tietosuoja-asetus hyväksyttiin huhtikuussa 2016.[74] Tietosuojauudistuksen tavoitteena oli toisaalta ajantasaistaa henkilötietojen suojaa koskevaa lainsäädäntöä, toisaalta laatia selkeät, johdonmukaiset ja joustavat säännöt henkilötietojen käsittelylle.[75]

Tietosuoja-asetus on osa digitaalisten sisämarkkinoiden kehittämistä. Sisämarkkinoiden digitalisoituminen on noussut keskeiseen asemaan jo vuosituhannen vaihteessa, kun vuonna 1995 säädettyä tietosuojadirektiiviä seurasi useita sisämarkkinoiden digitalisoitumiseen liittyviä direktiivejä.[76] Myös tietosuojauudistus on osa EU:n digitaalistrategiaa.[77] Digitaalistategiassa korostuu etenkin pyrkimys eurooppalaisten digitaalisten sisämarkkinoiden toimintaedellytysten vahvistamiseen.[78]

Keskeisenä syynä tietosuojalainsäädännön uudistamiseen oli henkilötietojen käsittelyyn vaikuttavaan tekniseen kehitykseen vastaaminen.[79] Sen lisäksi, että tekniset käsittelytavat ovat kehittyneet merkittävästi sitten henkilötietodirektiivin säätämisen, käsittely on hajautunut ja fragmentoitunut. Vielä direktiivin laatimisaikana oli käsittelyn osapuolilla tyypillisesti selkeät ja tarkkarajaiset roolit, ja käsittelytoimet olivat helposti tunnistettavissa, yksilöitävissä ja ilmoitettavissa viranomaiselle, kun taas nykypäivän henkilötietojen käsittelyssä niin käsittelytoimet kuin osapuolten roolitkin saattavat olla hyvinkin hankalasti määriteltävissä.[80]

---

[73] Korhonen 2003, s. 117.

[74] De Hert – Papakonstantinou 2016 s. 181, ks. myös WP 168. Samalla hyväksyttiin myös rikosasioita koskeva tietosuojadirektiivi. Tietosuojadirektiivi on osa tietosuojalainsäädäntöuudistusta, ja sitä sovelletaan henkilötietojen käsittelyyn rikosasioissa poliisien ja viranomaisten toiminnassa.

[75] Mouzakiti 2015, s. 46.

[76] Esimerkkinä mainittakoon direktiivit kuluttajansuojasta etäsopimuksissa (direktiivi 97/7/EY), sähköisestä kaupankäynnistä (direktiivi 2000/31/EY), sekä sähköisen viestinnän tietosuojasta (direktiivi 2002/58/EY).

[77] KOM (2010) 245, s. 13-14.

[78] KOM (2010) 245, s. 3.

[79] Uuden tekniikan vaikutusten huomioon ottamisesta ks. KOM(2010) 609, s. 3.

[80] De Hert ym. 2013, s.135. Roolien määrittelyyn liittyviä haasteita kuvastaa esimerkiksi tätä kirjoittaessa käsiteltävänä oleva Wirtschaftsakademie-tapaus (C-210/16), jossa on kyse Facebook-sivun ylläpitäjän mahdollisesta asemasta rekisterinpitäjänä. Rekisterinpitäjyyttä tarkasteltiin myös aiemmin mainitussa Google Spain -tapauksessa (C-131/12).

Toinen merkittävä syy tietosuojauudistukselle oli sääntely-ympäristön harmonisointitarve henkilötietodirektiivin jätettyä jäsenvaltioille melko laajan kansallisen liikkumavaran,[81] joka, kuten mainittua, johti toisistaan poikkeaviin lainsäädäntöratkaisuihin. Henkilötietodirektiivin implementoinnin on kritisoitu johtavan jäsenvaltioiden lainsäädännön fragmentoitumiseen, kun direktiivi oli implementoitu merkittävästi toisistaan poikkeavilla tavoilla.[82] Jäsenvaltioiden toisistaan merkittävästi poikkeavat tavat säännellä ja valvoa henkilötietojen suojaan liittyviä kysymyksiä johtivat niin yritysten kuin kuluttajienkin kannalta haasteellisiin tilanteisiin.[83] Lisäksi nykyaikaiset käsittelytoimet ovat yhä useammin luonteeltaan rajat ylittäviä, joten poikkeava sääntely-ympäristö ja yhtenäisyyden puute edellytti jokaisten maiden käytäntöjen tuntemista ja noudattamista sellaisilta toimijoilta, jotka haluaisivat käyttää sijoittautumisoikeuttaan toimiakseen useassa eri EU:n jäsenvaltiossa.[84] Sääntelymuodon vaihtumista direktiivistä asetukseen voidaankin pitää yhtenä keskeisimmistä muutoksista tietosuojauudistuksessa.[85]

Epäyhtenäisen lainsäädännön vaikutus toimintaedellytyksiin ilmenee myös runsaasta toimipaikan määräytymistä koskevasta oikeuskäytännöstä. Kysymystä käsiteltiin muun muassa Amazon-tapauksessa[86], jossa arvioitiin, minkä jäsenvaltion tietosuojalainsäädäntöä sovelletaan tapauksessa, jossa yhteen jäsenvaltioon sijoittautunut yritys tarjoaa palveluita toiseen jäsenvaltioon, sekä jäsenvaltioon asettautumiseen liittyviä kysymyksiä käsitelleissä Weltimmo- ja Google Spain -tapauksissa.[87] Tietosuoja-asetuksen myötä toimipaikan määräytymisen merkitystä, ja tätä myötä forum shopping -toiminta, jää vähemmän keskeiseksi yhtenäistyvän lainsäädännön myötä.

Asetuksella tavoiteltiin yhtäältä tehokkaampaa henkilötietojen suojaa, toisaalta sisämarkkinoiden toiminnan varmistamista etenkin digitaalisten sisämarkkinoiden osalta. Tavoitteidenasettelun jännitteelle on tyypillistä sisäänrakennettu ristiriitaisuus, jossa toisaalta

[81] De Hert ym. 2013 s. 134.
[82] Bräutigam 2012, s. 419, kritiikistä myös KOM (2012) 11, s. 4.
[83] Davies 2016, s. 293.
[84] KOM (2010) 609, s. 10. Esimerkiksi Googlen Street View -palveluun on suhtauduttu toisistaan poikkeavilla tavoilla eri jäsenvaltioissa. De Hert ym. 2013, s. 134. Esimerkiksi Saksassa palveluun kohdistui laajaa kritiikkiä, ja sen toiminnallisuuksia mukautettiin kansalliseen lainsäädäntöön sopivaksi. Mayer-Schönberger — Cukier 2013, s. 154. Suomessa palvelua käsiteltiin tietosuojalautakunnassa (14.07.2011 3/2011), joka asetti lupamääräykset palvelulle.
[85] De Hert – Papakonstantinou 2016, s. 182, Albrecht 2016, s. 287.
[86] VKI v. Amazon C-191/15.
[87] Weltimmo C-230/14, Google Spain C-131/12. Alueellisesta soveltuvuudesta laajemmin tietosuojatyöryhmän lausunto WP 179.

tavoitteena on yritystoiminnan edellytysten edistäminen, toisaalta sen ohjaaminen toivottuun suuntaan esimerkiksi asettamalla reunaehtoja tai karsimalla ei-toivottuja piirteitä.[88] Tämä jännite ilmenee myös tietosuoja-asetuksessa. Asetuksen tavoitteiden moninaisuus saattaa myös lisätä epäselvyyttä asetuksen tulkinnassa, kun asetuksella tavoitellaan henkilötietojen suojan lisäksi myös henkilötietojen vapaata liikkuvuutta, jota ei lähtökohtaisesti saa rajoittaa tai kieltää henkilötietojen suojan turvaamiseksi.[89] Tavoitteita tasapainotellaankin sisäisesti, jotta voidaan taata riittävä suoja yksilöille vaarantamatta kuitenkaan sisämarkkinoiden tehokasta toimintaa. Lisäksi tavoitteita tasapainotellaan myös ulkoisesti, jotta henkilötietojen suoja voidaan yhteen sovittaa muiden perusoikeuksien kanssa.

2.3 Osoitusvelvollisuuden muodostuminen tietosuojavaatimukseksi

Toimintaympäristön muuttuminen ja digitalisoitumiskehitys ovat eittämättä vaikuttaneet henkilötietodirektiivin turvaamaan henkilötietojen suojan tasoon. Henkilötietodirektiivin tavoitteet perusoikeuksien ja yksilön vapauksien tehokkaasta suojaamisesta sekä sisämarkkinoiden toiminnan turvaamisesta ovat kuitenkin yhä ajankohtaisempia. Henkilötietodirektiiviä on tulkittu laajasti, ja tulkinnalla on katsottu venytetyn rajoja henkilötietojen tehokkaan suojelun varmistamiseksi.[90] Tietosuojauudistuksen taustalla onkin pyrkimys varmistaa yksilöiden yhdenmukaiset ja tehokkaat keinot käyttää oikeuttaan henkilötietojen suojaan.[91]

Osoitusvelvollisuus nousi eurooppalaisen tietosuojaoikeudellisen keskustelun keskiöön tietosuojatyöryhmän vuonna 2009 antaman, yksityisyyden tulevaisuutta koskevan mietinnön, sekä tätä vuonna 2010 seuranneen osoitusvelvollisuutta käsitelleen mietinnön myötä.

Vuonna 2009 antamassaan mietinnössä tietosuojatyöryhmä katsoi, ettei henkilötietodirektiivin 17 artiklassa säädetty rekisterinpitäjän velvollisuus toteuttaa tarpeellisia teknisiä ja organisatorisia toimenpiteitä henkilötietojen suojaamiseksi laittomalta käsittelyltä ole käytännössä toiminut toivotulla tavalla.[92] Rekisterinpitäjien katsottiin sisäistäneen olemassa olevat tietosuojavelvoitteet puutteellisesti. Tietosuojatyöryhmän mukaan eri jäsenvaltioissa

[88] Tavoitteidenasettelun jännitteistä laajemmin Tala 2005, s. 163.
[89] Koillinen 2016, s. 579.
[90] De Hert — Papakonstantinou 2016, s. 180. Lain soveltamisympäristön muuttumisesta lain laatimisen jälkeen laajemmin Tala 2005, s. 169.
[91] KOM (2012) 9, s. 4.
[92] WP 168 s. 20.

esille tulleet tietosuoja-aiheiset kohut ja tietovuodot ovat osoittaneet puutteita niin teknisten järjestelmien kuin hallinnon tasolla.[93] Yhdeksi ratkaisuksi suojan kehittämiseksi tietosuojatyöryhmä esitti uusien periaatteiden, mukaan lukien osoitusvelvollisuuden ottamista osaksi eurooppalaista tietosuojalainsäädäntöä.[94]

Tietosuojatyöryhmä julkaisi seuraavana vuonna osoitusvelvollisuutta käsitelleen lausunnon, jossa määriteltiin osoitusvelvollisuuden tavoitteita, sisältöä sekä mahdollisia vaikutuksia, sekä asetettiin tavoitteeksi osoitusvelvollisuuden[95] tai siihen perustuvien ratkaisujen sisällyttäminen uusiutuvaan tietosuojalainsäädäntöön.[96] Lausunnossa tietosuojatyöryhmä toisti aiemman kantansa olemassa olevien keinojen riittämättömyydestä ja osoitusvelvollisuuden tarpeesta: henkilötietodirektiivin määräykset eivät ole käytännössä muodostuneet tehokkaiksi, todellisen suojan antaviksi mekanismeiksi.[97] Osoitusvelvollisuuden tarkoituksena ryhmän mukaan on rekisterinpitäjän aseman ja vastuun lisääminen ja tietosuojan tuominen "teoriasta käytäntöön."[98] Tietosuojatyöryhmä katsoi osoitusvelvollisuuden myös tukevan tietosuojaviranomaisten työtä auttamalla kohdistamaan voimavaroja mielekkäällä tavalla.[99]

Tietosuojatyöryhmä katsoi osoitusvelvollisuuden kannustavan rekisterinpitäjiä ottamaan käyttöön käytännöllisiä keinoja henkilötietojen suojan varmistamiseksi. Tavoitteena on ollut tuoda yleiset henkilötietojen käsittelyyn liittyvät periaatteet käytännöllisiksi, rekisterinpitäjän määrittelemiksi toimiksi, sekä vahvistamaan organisaatioiden tietosuojakulttuuria.[100] Toisaalta osoitusvelvollisuuden katsottiin muodostavan rekisterinpitäjälle velvollisuuden kyetä esittämään tosiasiallisia tuloksia, jättäen rekisterinpitäjälle vapauden valita — asetuksen muiden velvoitteiden rajoissa — tulosten saavuttamiseksi sopivat ja tarpeelliset keinot.[101]

Osoitusvelvollisuutta tarkasteltiin myös vuonna 2009 alkaneessa, eurooppalaisten tietosuojaviranomaisten sekä Center for Information Policy Leadership -ajatushautomon

---

[93] WP 168, s. 19.
[94] WP 168, s. 2.
[95] Lausunnossa osoitusvelvollisuudesta käytettiin vielä suomenkielistä termiä *tilivelvollisuus*, Tietosuoja-asetuksessa termi kääntyi muotoon *osoitusvelvollisuus*. Kyse on käännösmuutoksesta: esimerkiksi englanniksi velvollisuudesta on käytetty yhdenmukaisesti samaa nimitystä (*accountability*). Tietosuojatyöryhmä on myös itse todennut, että termiä on haastava kääntää yhdenmukaisesti eurooppalaisille kielille, WP 173, s. 8. Tutkielmassa käytetään asetuksen terminologiaa johdonmukaisuuden vuoksi.
[96] WP 173, s. 8.
[97] WP 173, s. 3.
[98] WP 173, s.3.
[99] WP 173, s. 17, ks. myös Alhadeff — Van Alsenoy — Dumortier 2012, s. 18.
[100] WP 173, s. 9.
[101] De Hert ym. 2013, s. 140.

(CNIL) aloittamassa Accountability Projects -sarjassa. Projektisarjassa tutkittiin osoitusvelvollisuutta keinona vastata teknologisen kehityksen sekä uusien liiketoimintamallien henkilötietojen suojalle aiheuttamiin haasteisiin.[102] Accountability projects -hankkeen aikana laaditut julkaisut tarkensivat osoitusvelvollisuuden määritelmää etenkin osoitusvelvollisuuden vuorovaikutuksellisuuden ja osoituksensaajan määrittelyn kautta.[103] Projektisarjan ensimmäinen, Irlannin tietosuojaviranomaisen (*Irish Data Protection Commissioner*) luotsaama ns. Galwayn projekti oli luonteeltaan kokeellinen, ja projektin yhteydessä laadittu mietintö olikin luonteeltaan lähinnä mietintömuotoinen hahmotelma osoitusvelvollisuudesta. Galwayn projekti näki haasteena sen, että vaikka osoitusvelvollisuuden merkitys tehokkaan tietosuojan toteutumiseksi on tunnistettu, ei sen sisältöä, kuten tapoja joilla osoitusvelvollisuuden noudattamisen voi osoittaa tai mitata, ole määritelty.[104] Galwayn projektiin osallistui yli 50 tahoa, mm. eurooppalaisia tietosuojaviranomaisia sekä liike-elämän edustajia.

Galwayn projektissa tarkastelu kohdistui nimenomaan osoitusvelvollisuuden elementteihin. Accountability projects -sarjan seuraava vaiheessa eli ns. Pariisin projektissa hahmoteltiin tarkemmin, minkälaisilla toimenpiteillä rekisterinpitäjä voisi noudattaa osoitusvelvollisuutta. Projektia koskeneessa mietinnössä tunnistetut elementit koskivat tietosuojakäytänteiden laatimista, hallinnollisia toimia ja tietosuojaan liittyviä henkilöstöresurssikysymyksiä, henkilökunnan kouluttamista, jatkuvaluonteista riskiarviointia ja -mitigaatiota, osoitusvelvollisuusohjelman hallintaa, kykyä vastata tietosuojapoikkeamiin, tietosuojakäytänteiden noudattamiseen liittyvää sisäistä valvontaa, sekä yksilöille tarjottavia vaikutuskeinoja poikkeamatilanteissa.[105]

[102] Alhadeff — Van Alsenoy — Dumortier 2012, s. 14.
[103] Butin —Chicote — Le Métayer 2014.
[104] Centre for Information Policy Leadership 2009, s. 1.
[105] Centre for Information Policy Leadership 2010, s. 6-7.

2.3. Osoitusvelvollisuuden sisältöön liittyvät tavoitteet

2.3.1. Rekisterinpitäjän vastuun tehostaminen

2.3.1.2. Rekisterinpitäjä käsittelystä määräävänä tahona

Tietosuojalainsäädännön peruslähtökohtana on, että vastuu henkilötietojen asianmukaisesta käsittelystä kohdistuu rekisterinpitäjään. Henkilötietojen suoja ei voi tehokkaasti toteutua, elleivät rekisterinpitäjät tee riittäviä toimia tehokkaan suojan toteuttamiseksi myös käytännössä.[106] Myös asetuksessa todetaan henkilötietoja käsittelevien sekä käsittelystä päättävien velvollisuuksien vahvistamisen ja täsmentämisen olevan välttämätöntä, jotta henkilötiedot tulevat asianmukaisesti suojatuksi.[107]

Rekisterinpitäjä on pääsääntöisesti se taho, joka hyötyy henkilötietojen käsittelystä, ja henkilötiedot ovatkin tulleet yhä arvokkaammaksi rekisterinpitäjille.[108] Toisaalta henkilötietojen käsittelystä seuraa usein henkilötietojen suojalle aiheutuvia riskejä, joiden mahdolliset seuraamukset, kuten esimerkiksi tietovuodot tai muut tietosuojaloukkaukset, ulottuvat rekisterinpitäjän lisäksi usein myös rekisteröityyn.[109] Rekisterinpitäjälle kyseessä on tyypillisesti maine- tai mahdollisesti sanktioriski, kun taas rekisteröidylle tietosuojaloukkauksesta saattaa aiheutua maineen vahingoittumisen tai taloudellisen vahingon lisäksi myös muita merkittäviä seuraamuksia.[110] Usein rekisteröity ei juurikaan voi vaikuttaa rekisterinpitäjän tekemiin tietosuojaratkaisuihin tai siihen, aktualisoituuko henkilötietojen käsittelystä seuraava riski, vaan nämä toimet ovat viime kädessä rekisterinpitäjän toteutettavissa.[111]

---

[106] Vastuun kohdistumisesta rekisterinpitäjään myös WP 169, s. 4.

[107] Tietosuoja-asetuksen resitaali 11.

[108] WP 173, s. 5, ks. myös. Mayer-Schönberger — Cukier 2013 s. 174.

[109] Iso-Britannian tietosuojavaltuutettu on blogissaan kuvannut riskin kantamista seuraavasti: *(...) The biggest change is around accountability. The new legislation creates an onus on companies to understand the risks that they create for others, and to mitigate those risks.*
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/gdpr-and-accountability/ [tieto haettu 1.1.2018].

[110] Esimerkkinä voidaan mainita tapaus, jossa Facebookin terrorismiaiheisten ryhmien moderointia tehneen työntekijän henkilöllisyys paljastui keskusteluryhmien osallistujille, altistaen moderaattorit mahdolliseen vaaraan. Kuchler 2017.

[111] Joissain käsittelytoimissa rekisteröity voi toki myös itse pyrkiä hallitsemaan yksityisyyttään tietosuojariskien minimoimiseksi. Kaikissa tilanteissa tämä ei kuitenkaan ole mahdollista, ja rekisteröidyn tekemistä toimista huolimatta haasteita saattaa syntyä muun muassa silloin, jos rekisterinpitäjä tekee jälkikäteisiä muutoksia esimerkiksi yksityisyysasetuksiin. Pitkänen — Tiilikka — Warma 2014, s.9.

Osoitusvelvollisuuden myötä rekisterinpitäjä on velvollinen osoittamaan, että toiminta on vaatimusten mukaista. On ilmeistä, että rekisterinpitäjä tuntee parhaiten oman toimintansa, eikä rekisteröity ole tyypillisesti osallisena käsittelyssä. Voidaankin katsoa, että rekisterinpitäjällä on lähtökohtaisesti rekisteröityä tai viranomaista paremmat edellytykset esittää käsittelyyn liittyvää näyttöä. Osoitusvelvollisuuden myötä myös ennakollisen valvonnan merkitys vähenee, ja toisaalta rekisterinpitäjän pitää nyt itse pystyä varmistumaan toiminnan lainmukaisuudesta ja osoittamaan se. Jatkossa ensimmäinen taho, joka tietosuojaedellytysten toteutumista valvoo, ei välttämättä ole tietosuojaviranomainen, vaan esimerkiksi yrityksen vaatimustenmukaisuudesta vastaava taho, kuten tietosuojavastaava.[112]

Myös rekisterinpitäjän näkökulmasta painopiste siirtyy ennakkoluonteisesta tarkastelusta riskilähtöiseen, koko käsittelyn elinkaaren kattavaan arviointiin: vaikka käsittelyn tuli toki aiemminkin olla lainmukaista läpi käsittelyn elinkaaren, painottuivat useat rekisterinpitäjältä edellytetyt, käsittelyn lainmukaisuutta tarkastelevat toimet — esimerkiksi ilmoitusvelvollisuus viranomaiselle tai edellytys rekisteriselosteen laatimisesta — pitkälti juuri käsittelyn alkupuolelle.[113] Osoitusvelvollisuus edellyttää koko käsittelynaikaisen lainmukaisuuden varmistamista, joten rekisterinpitäjän on syytä tarkastella sekä sitä, täyttääkö uusi tai suunnitteilla oleva käsittely lainsäädännön edellytykset, mutta myös sitä, onko jo käynnissä oleva käsittely edelleen tietosuojalainsäädännön vaatimusten mukaista.

2.3.1.1. Asymmetria rekisterinpitäjän ja rekisteröidyn välillä

Eurooppalaisen tietosuojalainsäädännön taustalla on korostunut tiedollisen itsemääräämisen konsepti.[114] Tiedollisen itsemääräämisoikeuden ydinsisältö on henkilön oikeus päättää omien tietojen käytöstään, tai ainakin vaikuttaa siihen.[115] Tiedollisen itsemääräämisoikeuden vaikutus tietosuojalainsäädännön luonteeseen on havaittavissa myös ajatuksessa, että tietojen käsittelyyn kuuluvat toimenpiteet tietojen keräyksestä sen säilytykseen ja lopulta poistoon ovat ennakoitavissa ja suunniteltavissa. [116]

[112] Partanen 2015, s. 169. Tietosuojavastaavan roolia käsitellään tarkemmin jaksossa 4.3.2.3.
[113] Tästä laajemmin Partanen 2015, s. 169.
[114] Kiss ym. 2015, s. 313.
[115] Albers 2014, s. 219-220. Albers kiinnittää huomioita siihen, miten käsite tiedosta on muotoutunut tietosuojalainsäädäntöön: tiedon katsotaan olevan rekisteröityä koskeva kuvaus todellisuudesta, jota kuitenkin voidaan käsitellä ja säännellä kuin omaisuusesinettä.
[116] Albers 2014, s. 211.

Tietosuojakysymyksissä korostuu tiedollisen asymmetrian hallinta: henkilötietojen käsittelylle on usein tyypillistä, että rekisteröidyllä on vähäisehköt mahdollisuudet saada tietoa omien tietojensa käsittelystä ja käsittelyn luonteesta, tarkoituksesta ja seuraamuksista.[117] Tätä rekisteröidylle epäedullista epätasapainoa pyritään lieventämään tietosuojalainsäädännön keinoin, ja ilman esimerkiksi informointi- ja läpinäkyvyysvaatimuksia rekisteröidyn edellytykset saada tietoa omien tietojensa käsittelystä olisivat heikommat.

Käsittelytoimien laajentuessa, monimutkaistuessa ja piiloutuessa tiedollinen asymmetria korostuu, kun rekisteröidystä tiedetään yhä enemmän, mutta rekisteröidylle käsittely jää hankalasti ymmärrettäväksi ja näkymättömäksi: läpinäkyvyyden sijaan rekisteröidyt "läpivalaistaan yksisuuntaisesti".[118] Henkilötietojen käsittelyn osapuolten välillä vallitseekin tyypillisesti vallan epätasapaino, kun laajan ja teknologisesti monitahoisen henkilötietojen käsittelyn hahmottaminen on haastavaa, ja monimuotoisten käsittelyjen rakenteellinen ja teknologinen ymmärtäminen edellyttää korkeaa osaamisen tasoa rekisteröidyiltä.[119]

Tiedolliseen asymmetriaan vaikuttaa myös tietojen hajautuminen tyypillisesti useisiin rekistereihin ja useille rekisterinpitäjille. Tällöin henkilö saattaa joutua sekä tunnistamaan asiaankuuluvan tai -kuuluvat rekisterinpitäjät sekä mahdollisesti asioimaan useamman rekisterinpitäjän kanssa.[120] Jos henkilötietojen suojan tosiasiallinen toteutuminen edellyttää rekisteröidyn tietoisuutta, aktiivisuutta sekä oma-aloitteisuutta, saattaa yksittäisen henkilön tietoa käsittelevien rekisterinpitäjien suuri määrä tehdä tehokkaan omien tietojen käsittelyn seurannan haastavaksi tai mahdottomaksi, kun omien henkilötietojen suojan toteutumisen varmistamiseksi joutuisi “valvomaan” useaa eri toimijaa. Tietosuojasääntelyn merkitys

[117] Koillinen 2013, s. 186. Tiedonkeruu sekä kerättyjen tietojen hyödyntämisen siirtyminen arkiseen ympäristöön hämärtää tiedonkeruun menetelmien ja vaikutusten näkyvyyttä entisestään. "Ubiikkiteknologian" eli kaikkialle ulottuvan tietoteknologian vaikutuksista tietosuojaymmärrykseen ks. laajemmin Karhula 2008, s. 39.

[118] Karhula 2008, s. 45.

[119] Matzner ym. 2016, s. 281. Yksittäisen teknologian lisäksi käyttäjän tulisi tuntea myös käsittelyn yhteydet ja käsittelykokonaisuuksiin liittyvät yhteisvaikutukset, tästä myös Karhula 2008, s. 50.

[120] Tästä myös Kallasvuo 2016, s.153. Toisaalta huomattava asymmetriasuhde muodostuu myös tilanteessa, jossa rekisterinpitäjälle tosiasiallisesti muodostuu lähestulkoon valta-asema rekisteröityyn nähden. Tästä on kyse esimerkiksi tapauksissa, joissa rekisterinpitäjällä on mittavat määrät rekisteröityä tai suurta rekisteröityjen joukkoa koskevia tietoja, etenkin jos tietojen keruu tapahtuu arkielämän ja yhteiskuntaan osallistumisen kannalta välttämättömien toimintojen yhteydessä: esimerkiksi hakukoneen käyttö tai matkapuhelimen omistaminen edellyttävät omien tietojen jakamista, jotta näitä palveluita voidaan käyttää, ja palveluiden ulkopuolelle jättäytyminen saattaa vaikeuttaa yhteiskunnallista ja sosiaalista osallistumista. Tähän nyky-yhteiskunnassa merkittävään asemaan kiinnitettiin huomiota Google Spain -tapauksessa (C-131/12, kohta 80). Vastaava valtasuhdeasetelma ilmenee myös Facebookia koskeneista Schrems-tapauksista (keskeisenä C-352/14), joiden saamassa mediahuomiossa on korostunut Daavid vastaan Goljat -retoriikka, ks. esim. Guardian 2014. Tästä myös Foegle 2016, s. 4.

korostuu etenkin tilanteissa, joissa tietojenkäsittely tapahtuu ilman rekisteröidyn vuorovaikutusta tai tietoisuutta.[121]

Osoitusvelvollisuuden myötä painopiste siirtyy rekisterinpitäjien itsenäisiin velvollisuuksiin. Tavoitteena on rekisteröityjen tehokas suojaaminen riippumatta siitä, ryhtyvätkö he proaktiivisesti toimenpiteisiin henkilötietojensa suojan turvaamiseksi.[122] Tällöin suojan taso ei edellytä rekisteröidyn osallistumista tai välttämättä edes tietoisuutta tai osaamista tietosuojalainsäädännön tuomista oikeuksista tai siitä, mitkä tahot käsittelevät tämän tietoja.[123] Siirtymää rekisteröidyn oikeuksille rakennetusta suojasta rekisterinpitäjän itsenäiseen vastuuseen on perusteltu esimerkiksi sillä, että henkilötietojen uudelleenkäyttötapojen yleistyessä big data -maailmassa tiedon keräysvaiheessa rekisteröidylle annetut tiedot eivät anna kattavaa kuvaa kaikista mahdollisista käyttötavoista, jolla tietoa tullaan sen elinkaaren aikana hyödyntämään, eivätkä myöskään aina kaikista niistä tahoista, jotka tietoa tulevat käyttämään.[124]

Rekisterinpitäjän vastuuseen keskittyvä malli suojaa etenkin niitä rekisteröityjä, joilla ei ole kykyä tai edellytyksiä valvoa henkilötietojensa suojan toteutumista. Esimerkiksi lasten ei voida olettaa kykenevän itse tunnistamaan tietosuojariskejä tai huomioimaan tietosuojaseikkoja palveluntarjoajaa valitessaan, joten rekisterinpitäjän vastuullisen toiminnan merkitys näiden tahojen henkilötietojen suojan tehokkaassa toteutumisessa korostuu.[125]

Todettakoon kuitenkin, että tietosuojauudistuksessa rekisteröidyn oikeuksien merkitys ei suinkaan ole heikentynyt, vaan asetuksen myötä henkilön oikeudet omiin henkilötietoihinsa vahvistuvat.[126] Nämä muutokset eivät kuitenkaan ole toisiaan poissulkevia, vaan osoitusvelvollisuus korostaa rekisterinpitäjän vastuuta käsittelyn lainmukaisuudesta riippumatta siitä, käyttääkö rekisteröity aktiivisesti oikeuksiaan.

---

[121] Kranenborg 2014, s. 229.
[122] Tästä myös WP 173, s. 8.
[123] Kiss — Szőke 2015, s. 312.
[124] Mayer-Schönberger — Cukier 2013, s. 173.
[125] Vastaavasti oletusarvoisen ja sisäänrakennetun tietosuojan merkitys korostuu silloin, kun rekisteröity ei itse kykene tekemään tietosuojaan liittyviä ratkaisuja. Koski 2017, s. 48.
[126] Tämä ilmenee esimerkiksi olemassa olevien oikeuksien tarkentumisesta (kuten esimerkiksi asetuksen tuoma mahdollisuus tarkastaa omat tiedot myös sähköisesti, tai henkilön oikeus saada aiempaa laajemmin tietoa omien tietojensa käsittelystä) sekä asetuksen tuomista täysin uusista oikeuksista (kuten rekisteröidyn oikeus siirtää omat tietonsa tietyissä tilanteissa rekisterinpitäjältä toiselle, ks. tietosuoja-asetuksen 20 artikla). Rekisteröidyn entistä aktiivisemman roolin mahdollistamisesta myös WP 168, s. 16.

2.3.2. Muuttuvan käsittely-ympäristön aiheuttamiin haasteisiin vastaaminen

2.3.2.1. Teknologianeutraaliuden toteuttaminen

Muuttuva teknologinen ympäristö sekä tiedon elinkaareen liittyvät kysymykset asettavat haasteita tietosuojalainsäädännön laatijalle, kun tieto ja sen käsittelytavat saattavat käsittelyn eri vaiheissa muuttaa muotoaan useaankin otteeseen, puhumattakaan yleisen käsittely-ympäristön ja käytettävissä olevan teknologian muutoksesta.[127] Tietosuojalainsäädännön säätämis- ja päivittämistarvetta on tyypillisesti perusteltu teknologisen kehityksen asettamiin haasteisiin vastaamisena: nykypäivän teknologinen ympäristö poikkeaa merkittävästi siitä ympäristöstä, jossa henkilötietodirektiivin keskeinen sisältö laadittiin. Samaa perustetta on käytetty aiempienkin tietosuojalainsäädäntöuudistusten yhteydessä.

Tulevaisuuteen suuntautuvan lainsäädännön laatiminen on haasteellista etenkin korkean teknologian ympäristössä. Lainsäätäjän pyrkimys teknologianeutraaliin lainsäädäntöön välittyy etenkin henkilötietodirektiivin periaatekeskeisyydestä: henkilötietodirektiivin periaatekeskeisyys on mahdollistanut tietosuojalainsäädännön mukautumisen teknologian kehityksen tuomaan merkittävään toimintaympäristön muutokseen.[128] Periaatelähtöisyys on tyypillistä tietosuojalainsäädännölle, jota onkin luonnehdittu "verrattain abstraktiksi".[129] Vastaavasti periaatelähtöisen lainsäädäntötavan on katsottu soveltuvan silloin, jos lainsäädäntöä laadittaessa ei tarkalleen tiedetä, millaisiin tilanteisiin sitä tullaan teknologisten muutosten myötä soveltamaan. Jos tietosuojalainsäädäntö laadittaisiin vahvasti kasuistiseksi ja yksittäiset tulkintatilanteet kattavaksi, edellyttäisi jatkuvasti muuttuvaan tietojenkäsittelyyn vastaaminen yksityiskohtaista ja raskasta, toistuvasti muutoksia edellyttävää lainsäädäntöä.[130] Toisaalta jotain tiettyä teknologiaa ennakoiva lainsäädäntö saattaisi jäädä kuolleeksi kirjaimeksi, jos teknologia ei leviä odotetusti eikä tarvetta sääntelylle muodostukaan.[131]

Tietosuoja-asetuksen osoitusvelvollisuus kohdistuu myös periaatteisiin.[132] Osoitusvelvollisuus on kirjoitettu verrattain avoimelle tasolle: se koskee lopputulosta, joka rekisterinpitäjän on saavutettava, eikä säännöksessä juurikaan määritellä yksityiskohtaisia keinoja sen

[127] Elinkaariajattelusta tarkemmin Saarenpää 2012, s. 330.
[128] WP 168, s. 12.
[129] Bygrave 2014, s. 3, Koillinen 2013 s. 172. Abstraktiudesta Saarenpää 2012, s. 330.
[130] Saarenpää 2012 s. 331.
[131] Huuskonen 2007, s. 436. Huuskonen mainitsee esimerkkeinä analogista tarkkapiirtotelevisiota koskevan sääntelyn sekä piirimallisuojan.
[132] Osoitusvelvollisuuden kohdistumista periaatteisiin käsitellään tarkemmin jaksossa 4.1.

saavuttamiseksi. Velvollisuuden dynaamisuus ja pyrkimys pysyä teknologian kehityksen mukana ovatkin olleet keskeisessä roolissa osoitusvelvollisuuden toiminnallisuutta määriteltäessä.[133] Kun rekisterinpitäjä velvoitetaan sekä valitsemaan nykyinen teknologia ja kustannukset huomioiden asianmukaiset keinot, että osoittamaan niiden tehokkuus ja ajanmukaisuus, ei lainsäätäjä joudu säädösvaiheessa määrittelemään käytännön toteutuskeinoja, jotka ovat usein aikaan sidottuja ja joskus nopeastikin vanhentuvia. Kun lainsäätäjä määrittelee lainsäädännön edellyttämän riittävän suojan tason, jää rekisterinpitäjän tehtäväksi valita kullakin hetkellä riittävät keinot, joilla tasoon päästään. Tällöin viime kädessä tuomioistuin arvioi keinojen kulloisenkin riittävyyden.

Teknologianeutraali, periaatekeskeinen lainsäädäntö edellyttääkin kultakin osapuolelta kykyä tunnistaa ongelmat eri asiayhteyksissä.[134] Toisaalta sääntelyn yleisluontoisuudesta ja tulkinnanvaraisuudesta johtuen rekisterinpitäjän mahdollisuudet saada etukäteen tietoa sallitun käsittelyn rajoista jäävät vähäisiksi, samalla kun jälkikäteisvalvonnan merkitys korostuu entisestään.[135] Rekisterinpitäjälle vaikeasti ennakoitavien säännösten sisältö saattaakin muotoutua vasta oikeuskäytännön — ja siten myös sanktiomaksujen soveltamiskäytännön — myötä.[136]

2.3.2.1. Rekisterinpitäjän hallinnollinen taakka ja valvontaviranomaisten resurssien tehokas kohdistaminen

Jotta osoitusvelvollisuus johtaisi keskeisen tavoitteensa mukaisesti tietosuojan tason paranemiseen, edellyttää se kiistatta toimenpiteitä rekisterinpitäjiltä. Asetuksen voimaantultua julkisessa keskustelussa on ollut esillä rekisterinpitäjiin kohdistuva, vaatimustenmukaisuuden toteuttamisesta johtuva hallinnollinen ja taloudellinen taakka.[137] Osoitusvelvollisuutta koskevassa mietinnössään tietosuojatyöryhmä ei kuitenkaan katsonut perustelluksi mahdollisia

[133] WP 173, s. 13.
[134] Saarenpää 2012 s. 428.
[135] Koillinen 2016, s. 579, tästä myös Koops 2014 s. 255.
[136] Koillinen 2016, s. 579.
[137] Liike-elämä on katsonut asetuksen uusien velvoitteiden lisäävän lainsäädännön noudattamisesta aiheutuvia compliance-kustannuksia merkittävästikin, tästä VN 2017, s. 6. Ks. toisaalta myös ICO 2017a, jossa Ison-Britannian tietosuojavaltuutetun toimisto katsoo tietosuoja-uudistuksen olevan "evoluutio eikä vallankumous", ja valtaosan velvoitteista olevan jo olemassa olevan tietosuojalainsäädännön mukaisia.

väitteitä osoitusvelvollisuuden rekisterinpitäjille tuomasta ylimääräisestä hallinnollisesta tai taloudellisesta taakasta.[138]

Tietosuojauudistuksen valmisteluvaiheessa tuotiin usein esille yleisellä tasolla tavoite vähentää rekisterinpitäjien hallinnollista taakkaa.[139] Hallinnollisen taakan keventyminen näkyy rekisterinpitäjille etenkin henkilötietodirektiivin 18 ja 19 artikloiden mukaisen ennakollisen ilmoitusvelvollisuuden poistumisena tietosuoja-asetuksen myötä.

Rekisterinpitäjien velvollisuutta ilmoittaa kaikista käsittelytoimista viranomaisille on kritisoitu vanhentuneeksi ja nykyaikaiseen henkilötietojen käsittelyyn sopimattomaksi.[140] Käsittelytoimiympäristö sekä etenkin suoritettavien käsittelytoimien määrä on epäilemättä kasvanut merkittävästi henkilötietodirektiivin laatimisen jälkeen. Velvollisuutta on pidetty myös rekisterinpitäjien taholta raskaana järjestelmänä, joka ei tuo todellista lisäarvoa rekisteröidyille.[141] Lisäksi ilmoitusvelvollisuuden osalta direktiivissä oli kansallista liikkumavaraa, ja ilmoitusvelvollisuus onkin implementoitu eri tavoin.[142]

Ilmoitusvelvollisuuden poistuminen vähentää useissa jäsenvaltioissa toimivan rekisterinpitäjän tarvetta täyttää toisistaan poikkeavia kansallisia vaatimuksia, eli hallinnollisen taakan vähentymisen lisäksi muutoksella voidaan katsoa olevan myös sisämarkkinoita tukeva vaikutus. Kansallisten lainsäädäntöjen yhtenäisyys johtaa toki siihen, että samankaltainen osoitusvelvollisuuden täyttämisen taso tulisi riittää kaikissa jäsenvaltioissa.

Ennakkoluonteisen ilmoitusvelvollisuuden poistuessa tietosuoja-asetuksessa uutena velvoitteena on rekisterinpitäjän velvollisuus ilmoittaa tietosuojaloukkauksesta.[143] Muutos kuvaa tietosuojavalvonnan painospisteen siirtymistä etukäteisvalvonnasta käsittelynaikaisen

[138] WP 173, s. 10. Komissio katsoo vastaavasti, ettei uuden asetuksen tarkoituksena ole lisätä rekisterinpitäjien hallinnollista taakkaa, vaan luoda takeita ja mekanismeja, jotka samanaikaisesti tehostavat tietosuojasääntöjen noudattamista sekä vähentävät ja yksinkertaistavat hallinnollisia muodollisuuksia. KOM (2010) 609, s. 12.

[139] Tästä esim. KOM(2010) 609, s. 10-11.

[140] Bräutigam 2012, s. 435.

[141] De Hert — Papakonstantinou 2009, s. 139, KOM(2010) 609, s. 19.

[142] Direktiivi mahdollisti kansallisen poikkeamisen rekisterinpitoilmoituksista, jonka johdosta Suomessa ennakollista ilmoitusta käsittelystä on edellytetty vain tiettyjen keskeisten rekisterien (esim. luottotietorekisteri) osalta. Muiden, tavanomaisempien rekisterien jättämistä ilmoitusvelvollisuuden ulkopuolelle perusteltiin juuri tarpeettoman byrokratian välttämisellä. Lisäksi huomioitiin käytännön tietoturvariskit, joita ilmoitusvelvollisuuden toteuttaminen saattaisi aiheuttaa. Saarenpää 2012, s. 335.

[143] Vastaava ilmoitusvelvollisuus on jo sähköisen viestinnän tietosuojadirektiivissä, mutta velvoite koskee vain telealaa. Yleisen ilmoitusvelvollisuus yhtenäistää oikeustilaa tietosuojaloukkausilmoitusten osalta. Tästä myös KOM(2010) 609 lopullinen, s. 6-7.

lainmukaisuuden varmistamiseen.[144] Lisäksi asetus edellyttää rekisterinpitäjää ennakkokuulemaan tietosuojaviranomaista tietyissä korkean riskin käsittelytilanteissa.[145]

Painopisteen siirtymästä heijastuukin myös riskilähtöisyys: sen sijaan, että viranomaisille tulisi ilmoittaa kaikesta käsittelystä, saa rutiinikäsittelyä suorittaa jatkossa ilman erillistä ilmoitusvelvollisuutta, ja viranomaisiin on oltava yhteydessä vain korkean riskin käsittelyn yhteydessä tai tietovuotoilmoituksella riskin aktualisoiduttua.

Tietosuoja-asetuksen edellyttämien, osoitusvelvollisuuteen liittyvien sekä muiden hallinnollisten toimenpiteiden kustannuksista rekisterinpitäjille on tätä kirjoittaessa vain alustavia arvioita.[146] Jää nähtäväksi, toteutuuko tavoite asetuksen hallinnollista taakkaa vähentävästä vaikutuksesta, vai siirtyykö hallinnollinen taakka ilmoitusvelvollisuuden poistuessa osoitusvelvollisuuden sekä muiden tietosuoja-asetuksen uusien vaatimusten toteuttamiseen.

[144] Partanen 2015, s. 169.
[145] Ennakkokuuleminen liittyy vaatimukseen laatia tietosuojan vaikutustenarviointi tietyissä käsittelytilanteissa. Vaikutustenarviointia käsitellään tarkemmin kohdassa 4.3.2.2.
[146] Alustavista yritysvaikutuksista ks. esim. VN 2017, s. 6.

3. Osoitusvelvollisuuden luonne ja tasot

3.1. Osoitusvelvollisuuden sisältö

Osoitusvelvollisuutta on usein kuvattu moniulotteiseksi, hankalasti määriteltäväksi ja epätäsmälliseksikin.[147] Tietosuojatyöryhmän osoitusvelvollisuutta koskevassa mietinnössä osoitusvelvollisuus jäsennetään kahteen elementtiin:

> 1) rekisterinpitäjän velvollisuuteen *tehdä asianmukaiset ja toimivat toimet* henkilötietojen käsittelyyn liittyvien periaatteiden toteuttamiseksi, ja
> 2) tämän velvollisuuteen *kyetä osoittamaan, että edellä mainitut toimet on toteutettu*.[148]

Osoitusvelvollisuuden lähtökohtana jo OECD:n periaatteissa on ollut vastuun kohdistuminen nimenomaisesti rekisterinpitäjään. Rekisterinpitäjän toiminnan lainmukaisuuden on aiemmin kuvattu jääneen "sokean luottamuksen" varaan: tiedetään, että rekisterinpitäjän tulee kyllä noudattaa tälle osoitettuja velvollisuuksia, mutta tällä ei ole lähtökohtaisesti velvollisuutta osoittaa toimintansa lainmukaisuutta, kun taas osoitusvelvollisuuden tuomaa vastuuta on kuvailtu "todistettuna luottamuksena".[149] Tietosuojatyöryhmän jäsentelyä velvollisuuteen tehdä toimet ja kyetä osoittamaan niiden toteutus voidaankin siis tarkastella kriittisesti: ensimmäinen elementti, eli lainsäädännön velvoitteiden noudattaminen, ei sinänsä kuulu osoitusvelvollisuuteen, vaan velvollisuuden tosiasiallinen sisältö kohdistuu nimenomaan toiseen elementtiin eli toiminnan lainmukaisuuden osoittamiseen.[150]

Osoitusvelvollisuutta tarkastellut Bennett[151] jakaa osoitusvelvollisuuden kolmeen elementtiin:

> *Osoitusvelvollisuus periaatteiden tasolla (accountability of policy)*, jolla rekisterinpitäjä osoittaa määritelleensä asianmukaisesti laaditut tietosuojaperiaatteet tai vastaavat käytännesäännöt: tällaista osoitusvelvollisuutta voidaan pitää

[147] Ks. esim. Alhadeff — Van Alsenoy — Dumortier 2012, s. 3; Butin — Le Métayer 2014, s. 2.
[148] WP 173, s.9.
[149] Alkuperäiskielellä “blind trust” ja “proven trust”. De Hert 2012, s. 199.
[150] Tietosuojatyöryhmä toteaa lausunnossaan valtaosan osoitusvelvollisuuteen kuuluvista velvoitteista — lainsäädännön velvoitteiden noudattamisen käsittelytoiminnassa — olevan jo olemassa olevia velvoitteita, joita osoitusvelvollisuus vain tarkentaa. WP 173, s. 10.
[151] Bennett 2010, s. 6.

rekisterinpitäjän keinona ilmaista aikomuksensa ("declaration of intent"), jota voidaan osoitusvelvollisuuden myötä verrata lainsäädännön edellytyksiin.[152]

Osoitusvelvollisuus menettelyjen tasolla (accountability of procedures), joilla rekisterinpitäjä osoittaa organisatorisia toimia, joilla edellämainittuja tietosuojaperiaatteita ja muita tietosuojalainsäädännön vaatimuksia pannaan täytäntöön: kyse voi olla esimerkiksi tietosuojan vaikutustenarviointien laatimisesta, henkilökunnan koulutuksesta, tai muista organisatorisista toimista.

Osoitusvelvollisuus käytäntöjen tasolla (accountability of practice) kuvaa edellisen tason toimenpiteiden tosiasiallista toteutumista, eli sen merkitys muodostuu tietosuojaperiaatteita toteuttavien menettelyjen jälkikäteisestä dokumentoinnista ja todistamisesta.

Bennettin tarkoittamalla ensimmäisellä tasolla rekisterinpitäjä peilaa lainsäädännön vaatimuksia omaan toimintaansa ja laatii näiden vaatimusten perusteella toimintaansa sitovat tavoitteet. Toisella tasolla rekisterinpitäjä tunnistaa ensimmäisen tason toteuttamiseksi tarpeen olevat toimet ja tuo ensimmäisen tason tavoitteet menettelyjen tasolle. Kolmas taso takaa osoitusvelvollisuuden koko laajuuden toteutumisen.[153]

Näistä periaatteiden ja menettelyjen taso vastaa tietosuojatyöryhmän määrittelemää ensimmäistä elementtiä: rekisterinpitäjän on tunnistettava ja määriteltävä keinot, joilla se toteuttaa tietosuoja-asetuksen mukaisia periaatteita, sekä toimeenpantava nämä toimet periaatteiden toteuttamiseksi. Myös tällöin kyse on lainsäädännön velvoitteiden noudattamisesta, eikä varsinaisesti niiden noudattamisen osoittamisesta, eli näillä tasoilla osoitusvelvollisuudella ei ole varsinaista lisäarvoa lainsäädännön edellytyksiin nähden. Siten osoitusvelvollisuudessa on tältä osin kyse olemassaolevien velvoitteiden tosiasiallisen noudattamisen edellytyksestä, eikä niinkään kokonaan uudesta velvoitteesta.[154]

Velvollisuus kyetä osoittamaan että toimet on toteutettu, luo taaksepäin katsovan, jo toteutuneita menettelyjä koskevan edellytyksen, ja vastaa Bennettin osoitusvelvollisuutta käytäntöjen tasolla. Osoitusvelvollisuuden keskeisimmäksi sisällöksi muodostuukin selvitysvelvollisuus tehdyistä toimenpiteistä sekä etenkin näyttövelvollisuus esitettyjen

[152] Butin — Le Métayer 2015, s. 2.
[153] Butin — Le Métayer 2015, s. 2.
[154] WP 173, s. 10.

toimenpiteiden tehokkuudesta.[155] Voidaankin sanoa, että osoitusvelvollisuus konkretisoituu vasta käytäntöjen tasolla.

3.2. Osoitusvelvollisuuden itsenäinen merkitys

Tietosuoja-asetusta valmisteltaessa on useaan kertaan todettu osoitusvelvollisuuden olevan itsenäinen velvollisuus.[156] Jos osoitusvelvollisuus kuitenkin konkretisoituu näyttövelvollisuutena toiminnan lainmukaisuudesta, voidaan kysyä, onko osoitusvelvollisuudella omaa, itsenäistä sisältöä, vai onko se pelkästään Troijan hevonen, joka pitää sisällään muut tietosuojaperiaatteet ja -vaatimukset. Edellyttääkö osoitusvelvollisuuden rikkominen myös jonkin muun tietosuojavaatimuksen rikkomista, vai voiko osoitusvelvollisuutta rikkoa, vaikka toiminta olisi muutoin täysin asetuksen edellytysten mukaista?

Tietosuoja-asetuksessa säädetään laajasti asetuksen noudattamatta jättämisen seuraamuksista ja moniportaisista sanktioista, ja etenkin asetuksen mahdollistamat hallinnolliset sanktiomaksut ovat saaneet merkittävästi huomiota tietosuoja-asetukseen liittyvässä julkisessa keskustelussa.[157] Asetuksen rikkomisesta määrättävissä oleva sanktio on jaettu määrältään kaksiportaiseksi: sanktion enimmäismäärä on rikotusta tietosuoja-asetuksen velvoitteesta riippuen joko 10 miljoonaa euroa tai 2 % yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta liikevaihdosta sen mukaan, kumpi näistä määristä on suurempi, tai 20 miljoonaa tai vastaavasti 4 %. Henkilötietojen käsittelyä koskeviin periaatteisiin kohdistuvaan, 5 artiklan osoitusvelvollisuuteen kohdistuu korkeampi enimmäismäärä. Lisäksi sisäänrakennetun ja oletusarvoisen tietosuojan periaatteen rikkomista koskee matalampi hallinnollisen sanktion enimmäismäärä. Osoitusvelvollisuus on siis yksi velvoitteista, joiden rikkominen voi johtaa hallinnolliseen sanktioon, eli rekisterinpitäjälle voi koitua seuraamuksia osoitusvelvollisuuden rikkomisesta.[158]

---

[155] Tietosuojatyöryhmän mietinnössä tiivistetään selvitys- ja näyttövelvollisuutta: ”painotus on kuitenkin sen osoittamisessa, että vastuuta kannetaan ja että tämä on todennettavissa”, WP 173, s. 7.

[156] Esimerkiksi Buttarelli 2017, s. 2.

[157] Esimerkiksi tietosuojavaltuutettu Reijo Aarnio on käsitellyt blogikirjoituksessaan “Totuus hallinnollisista sanktioista” sanktionuhkaa http://www.tietosuoja.fi/fi/index/blogi/6IUtCELFH/2017/bCDF80rfD.html.stx [tieto haettu 1.1.2018].

[158] Toisaalta laiminlyönneistä, joihin ei sovelleta hallinnollisia sakkoja, voidaan määrätä muita seuraamuksia. VAHTI-raportti, s. 30. Mainittakoon, että sanktio koskee vain 5 artiklan periaatteisiin kohdistuvaa osoitusvelvollisuutta, eli 24 artiklan yleisvelvoitteen rikkomisesta ei voida määrätä sanktiota: sanktiomahdollisuus oli esillä asetuksen valmisteluvaiheessa, muttei päätynyt lopulliseen asetustekstiin. Asetus

Asetuksessa ei kuitenkaan oteta kantaa siihen, mikä osoitusvelvollisuuden suhde on muihin tietosuojaperiaatteisiin tai miten vastuu osoitusvelvollisuuden rikkomisesta suhtautuu muiden tietosuojaperiaatteiden rikkomiseen.[159] Osoitusvelvollisuutta koskevassa mietinnössään tietosuojatyöryhmä on katsonut, että sanktio osoitusvelvollisuuden rikkomisesta tulisi määräytyä tietosuojaloukkauksen lisäksi ylimääräisenä sanktioelementtinä.[160]

Koska osoitusvelvollisuuteen kuuluu sisäänrakennettuna rekisterinpitäjän velvollisuus noudattaa asetusta, jotta tämä voisi ylipäätään osoittaa noudattaneensa sitä, vaikuttaisi siltä, että osoitusvelvollisuus voi tosiasiallisesti ja koko laajuudeltaan tulla noudatetuksi vain silloin, kun rekisterinpitäjä sekä noudattaa asetusta että kykenee osoittamaan tämän.

Sen sijaan kysymys siitä, voiko kyseeseen tulla pelkän osoitusvelvollisuuden rikkominen, vaikuttaisi olevan lähinnä teoreettinen. Osoitusvelvollisuuden itsenäinen merkitys saattaa kuitenkin ajankohtaistua sen toiminnallisen roolin kautta: tietosuojatyöryhmä on katsonut osoitusvelvollisuuden tulevan kyseeseen itsenäisenä velvoitteena ainakin niissä tilanteissa, joissa rekisterinpitäjä ei luovuta tietoa valvovan viranomaisen pyynnöstä. Tämä osoitusvelvollisuuden rikkominen muodostaisi välittömän syyn ryhtyä toimenpiteisiin rekisterinpitäjää kohtaan riippumatta siitä, onko muita tietosuojaperiaatteita rikottu.[161] Tällöin osoitusvelvollisuuden merkityksen voidaan katsoa kohdistuvan tehdyistä toimenpiteistä ulkopuoliselle taholle kertomiseen.

3.3. Osoitusvelvollisuus vuorovaikutussuhteena

3.3.1. Osoitusvelvollisuuden vuorovaikutuksellisuus ja osoituksen kohdistuminen

Osoitusvelvollisuudella kohdistetaan velvollisuuksia rekisterinpitäjälle. Vastuun kohdistuminen juuri rekisterinpitäjään on ilmeistä, ja se käy suoraan ilmi osoitusvelvollisuuden sanamuodosta.[162] Osoitusvelvollisuus on kuitenkin luonteeltaan kerronnallinen, eli osoitus

ei ota kantaa 5 artiklan ja 24 artiklan rikkomisen eroavaisuuteen tai siihen, johtaako 24 artiklan rikkominen automaattisesti siihen, että myös 5 artiklaa on rikottu. 5 artiklan ja 24 artiklan sisältöä käsitellään tarkemmin jaksossa 4.1. ja 4.2.

[159] Greenleaf 2013, s. 240.

[160] WP 173, s. 17.

[161] WP 173, s. 16.

[162] Osoitusvelvollisuuden kohdistumista rekisterinpitäjään voi pitää kiistattomana: niin OECD:n tietosuojasuositus, tietosuojatyöryhmän valmistelevat materiaalit, Accountability Projects -mietinnöt, kuin tietosuoja-asetuksen teksti kohdistavat vastuun nimenomaisesti rekisterinpitäjään. Henkilötietojen käsittelijän vastuuseen liittyvät kysymykset jäävät tutkielman kohteen ulkopuolelle.

osoitetaan, laaditaan ja toimitetaan jollekin toiselle taholle. Kyse ei siis ole tyhjiössä toimivasta velvollisuudesta, vaan siihen kuuluu sisäänrakennettu vuorovaikutussuhde ja yleisö: velvollisuus kohdistuu vastuussa olevaan tahoon eli rekisterinpitäjään, joka vastaa toiminnastaan toiselle taholle.[163]

Sen sijaan tahoa, kenelle osoitetaan, eli "osoituksen" vastaanottajaa ja yleisöä, ei määritellä asetuksessa. Toiminnan vaatimustenmukaisuutta valvova kansallinen viranomainen on eittämättä keskeinen taho, jolle rekisterinpitäjä kohdistaa osoituksensa. Tietosuojatyöryhmän yksityisyydensuojan tulevaisuutta koskeneessa mietinnössä osoitusvelvollisuutta on katsottu toteutettavan *ulkoisille sidosryhmille*, joista kansallinen tietosuojaviranomainen on vain yksi osoitusvelvollisuutta vastaanottavista osapuolista.[164]

Osoitusvelvollisuus ei sellaisenaan anna rekisteröidylle oikeutta vaatia rekisterinpitäjää osoittamaan suoraan rekisteröidylle noudattavansa tietosuojavaatimuksia, vaan rekisteröidyn on käännyttävä tietosuojaviranomaisten puoleen puutteita epäillessään. Voidaan kysyä, pelkistyvätkö osoitusvelvollisuuden vaikutukset yksinomaan rekisterinpitäjän ja valvovan viranomaisen keskinäiseen suhteeseen.[165]

Toisaalta osoitusvelvollisuuden tuomista tietosuoja-asetuksen tasolle on perusteltu nimenomaan siirtymänä rekisterinpitäjän itsenäistä vastuuta korostavaan malliin, joka ei edellytä rekisteröidyn aktiivisuutta henkilötietojen tehokkaan suojan toteuttamiseksi. Tällöin kerronnallisuuden vaikutukset välittyvät rekisteröidylle lähinnä välillisesti.

3.3.2. Osoitusvelvollisuus suhteessa valvontaviranomaiseen

Tietosuojaviranomaisen rooli rekisterinpitäjän osoitusvelvollisuuden vastinparina on kiistaton. Toisin kuin aiemmassa lausunnossaan, tietosuojatyöryhmä ei osoitusvelvollisuutta koskevassa lausunnossaan nosta esille kysymystä siitä, kenelle osoitusvelvollisuudella osoitetaan, vaan tarkastelee suoraan sitä, miten osoitusvelvollisuus vaikuttaa valvontaviranomaisen rooliin.[166]

---

[163] Alhadeff — Van Alsenoy — Dumortier 2012, s. 5.

[164] "*The accountability principle would require data controllers to have the necessary internal mechanisms in place to demonstrate compliance to external stakeholders, including national DPAs,"* ks. WP 168, s. 20.

[165] Huomattakoon, että tuomioistuimessa osoitusvelvollisuus saattaisi tulla esille myös editiovelvollisuuden kautta.

[166] WP 173, s. 16.

Osoitusvelvollisuus ei aktualisoidu vasta viranomaisen ottaessa yhteyttä rekisterinpitäjään. Käytännössä osoitusvelvollisuuden tehokas toteuttaminen edellyttääkin dokumentaation laatimista ja sen olemassaoloa riippumatta siitä, pyytääkö kukaan taho sitä nähdäkseen.[167] Osoitusvelvollisuutta ei voikaan pelkistää vain rekisterinpitäjän velvollisuuteen toimittaa nimenomaisia dokumentteja valvontaviranomaiselle pyynnöstä.[168] Osoitusvelvollisuus ei sinänsä myöskään kohdistu mihinkään yksittäiseen käsittelytoimeen, vaan vaatimustenmukaisuus on kyettävä osoittamaan missä käsittelyn vaiheessa tahansa.[169]

Valvontaviranomaisten oleelliseksi tehtäväksi muodostuu tarvittaessa tarkastaa ja tutkia rekisterinpitäjän osoitusvelvollisuudella kertoman kuvauksen totuudenmukaisuus: osoitusvelvollisuus toisaalta antaa näkyvyyttä "näkymättömille" tietosuojaan liittyville rekisterinpitäjän toimenpiteille, toisaalta kuvaa valvontaviranomaiselle rekisterinpitäjän tavoitteita sekä omaa ymmärrystä käsittelytoimiin liittyen.[170]

Tietosuojatyöryhmä kiinnittää huomiota myös osoitusvelvollisuuden yleiseen positiiviseen vaikutukseen tietosuojavaatimusten noudattamisen valvonnalle: osoitusvelvollisuus mahdollistaa viranomaisille keinon tietosuojavaatimusten noudattamisen tason tarkkailulle. Osoitusvelvollisuuden valvonta ei edellytä esimerkiksi epäilystä tietosuojavelvoitteiden rikkomisesta, vaan tiedot on annettava pyynnöstä.[171] Näin tietosuojaviranomainen saa käytettäviinsä tietoa tietosuojavaatimusten noudattamisesta, mikä mahdollistaa tietosuojavaatimusten noudattamisen valvonnan mielekkäämmän kohdentamisen, kun lainvalvontaresurssit voidaan kohdentaa esimerkiksi sellaisille toimialoille tai toimijoille, joiden toiminnassa ilmenee ilmeisiä puutteita.[172]

Kiihtyvä teknologinen kehitys ja laskentatehon kasvu ovat vaikuttaneet merkittävästi henkilötietojen käsittelytoimien määrään ja tätä myötä myös viranomaisten mahdollisuuksiin

---

[167] Esimerkiksi seloste käsittelytoimista on laadittava ja ylläpidettävä riippumatta siitä, pyytääkö mikään taho sen laatimista tai toimittamista. Seloste toimitetaan viranomaisille pyynnöstä.

[168] Coudert 2014, s. 81. Toisaalta nimenomaisella dokumentaatiolla on myös keskeinen merkitys, esimerkiksi henkilötietoihin kohdistuneen tietovuodon sattuessa rekisterinpitäjän tulee toimittaa 33(5) artiklan mukainen dokumentaatio viranomaisille, jotta nämä voivat selvittää, toteutuiko ilmoitusvelvollisuus artiklan edellytysten mukaisesti.

[169] Partanen 2015, s. 169.

[170] Coudert 2014, s. 81-82. Osoitusvelvollisuus liittyykin olennaisesti tietosuojaviranomaisten valvontatoimivaltaan, tästä WP 173 s. 16.

[171] WP 173, s. 17.

[172] WP 173, s. 17. Vastaavasti osoitusvelvollisuus saattaa helpottaa valvonnan kohdistamista tiettyihin toimijoihin sellaisilla toimialoilla, joissa käsitellään tietosuojan kannalta korkean riskin tietoja, kuten esimerkiksi terveydenhuoltopalveluissa tai finanssialalla.

varmistaa tietosuojavaatimusten noudattaminen. Teknisen kehityksen vaikutus lieneekin yksi syy sille, miksi osoitusvelvollisuus on otettu lain tasoiseksi vaatimukseksi juuri nyt: voitaneen olettaa henkilötietojen käsittelyn yleistymisen jatkuvan myös tulevaisuudessa tietoyhteiskunta- ja digitalisaatiokehityksen myötä, joten valvontaviranomaisten resurssien tehokkaampi kohdistuminen lienee perusteltu tavoite henkilötietojen suojan riittävän toteutumisen takaamiseksi.

3.3.3. Osoitusvelvollisuus suhteessa rekisteröityyn

Henkilötietojen käsittely tehdään usein rekisterinpitäjän suljettujen ovien takana, eikä käsittelyn luonne, tai aina sen tapahtuminenkaan, välity aina rekisteröidylle.[173] Käsittelyn suljetun luonteen käytännön vaikutuksia rekisteröidylle havainnollistaa aiemmin käsitelty I v. Suomi -tapaus, jossa EIT nosti esille todistustaakan jakoon liittyvät haasteet. Tapauksessa valittaja ei ollut kyennyt näyttämään syy-yhteyttä yksityisyytensä suojan vaarantumisen ja tapauksessa kyseessä olleen teknisen järjestelmän puutteiden välillä. Tuomioistuin totesi, että todistustaakan jättäminen hakijalle sivuuttaa tapauksessa rekisterinpitäjänä toimineen tahon tunnetut puutteet henkilötietojen käsittelyssä.[174]

Kun osoitusvelvollisuus kohdistuu rekisterinpitäjään, ei rekisteröidyn tarvitse kyetä itsenäisesti osoittamaan puutteita käsittelyssä, johon rekisteröidylle ei ole pääsyä tai näkyvyyttä.[175] Toisaalta osoitusvelvollisuus ei sellaisenaan tuo rekisterinpitäjälle velvollisuuksia rekisteröidyn suuntaan: tosin rekisterinpitäjän on kyettävä osoittamaan viranomaisille, että esimerkiksi rekisteröityjen oikeuksien toteuttamista koskevista toimenpiteistä on huolehdittu asianmukaisesti. Voidaankin kysyä, millä tasolla "todistettu luottamus" tosiasiallisesti kulkeutuu rekisteröidylle asti, kun rekisterinpitäjän ei lähtökohtaisesti tarvitse julkaista osoitusvelvollisuuteen liittyvää dokumentaatiota tai muita lopputuloksia, eli konkreettinen vaikutus rekisteröityjen luottamukselle jää epäselväksi.[176]

Rekisteröidyn ensisijaiset keinot saada tietoa käsittelystä eivät varsinaisesti liity osoitusvelvollisuuden toteuttamiseen, vaan ne ovat osoitusvelvollisuudesta itsenäisiä

[173] De Hert ym. 2013, s. 141.
[174] I v. Suomi, kohta 44. Tästä tarkemmin De Hert 2011, s. 101.
[175] De Hert ym. 2013, s. 141.
[176] Huomattakoon kuitenkin rekisterinpitäjän henkilötietojen käsittelyyn liittyvä, osoitusvelvollisuudesta sinänsä irrallinen informointivelvoite.

oikeuksia.[177] Toisaalta etenkin asetuksen velvoitteeseen toimittaa rekisteröidylle tietoa käsittelystä[178] sisältyy osoitusvelvollisuuteen yhteydessä olevia elementtejä, sillä osa rekisteröidylle kerrottavista tiedoista kuvaavat tosiasiallisesti myös käsittelyn lainmukaisuutta.[179] Myös tietosuojatyöryhmä on katsonut käsittelytoimien läpinäkyvyyden olevan edellytys osoitusvelvollisuuden tosiasialliselle toteutumiselle,[180] tai ainakin läpinäkyvyyden rekisteröityä ja yleistä yleisöä kohtaan tukevan osoitusvelvollisuuden toteuttamista.[181] Läpinäkyvyyttä voidaankin toteuttaa rekisteröidyn yleisen informoinnin lisäksi esimerkiksi läpinäkyvillä sisäisillä valitustenkäsittelyprosesseilla sekä vuosijulkaisuilla.[182]

Läpinäkyvyyttä voidaan tarkastella myös suhteessa rekisteröidyn mahdollisuuksiin käyttää muita tietosuojalainsäädännön takaamia oikeuksiaan: rekisteröidyn tiedonsaantioikeuden kautta toteutettava läpinäkyvyys edeltää muita oikeusturvakeinoja, muut keinot saattavat jäädä tosiasiallisesti merkityksettömiksi, jos rekisteröity ei ole tietoinen käsittelyn luonteesta tai sen tapahtumisesta. Asianmukaisesti toteutettu informointi ja läpinäkyvyys voivatkin olla keinoja osoittaa, että rekisterinpitäjä on pyrkinyt varmistamaan rekisteröidyn mahdollisuudet olla tietoinen käsittelystä ja käyttää tietosuojalainsäädännön mukaisia rekisteröidyn oikeuksia.

Keskeisin osoitusvelvollisuuden merkitys rekisteröidylle lieneekin, että velvollisuus osoittaa toiminnan lainmukaisuus siirtyy rekisterinpitäjälle. Toisaalta jos osoitusvelvollisuus osoittautuu tehokkaaksi instrumentiksi henkilötietojen suojan toteuttamiseen, välittyy kohonnut suojan taso rekisteröidylle riippumatta siitä, että rekisteröity ei itse olekaan osoitusvelvollisuuden varsinainen vastaanottaja.

Osoitusvelvollisuuden vuorovaikutussuhteessa rekisteröity onkin lähinnä hyötyjän, ei itse osoitusten vastaanottajan roolissa. Tämän lisäksi osoitusvelvollisuudella voi olla myös funktionaalinen merkitys etenkin läpinäkyvyyden osalta. Kun rekisterinpitäjän tulee kyetä

---

[177] Keskeisimmät läpinäkyvyyden toteutustavat, kuten rekisteröidyn informointi sekä rekisteröidyn tarkastusoikeus, ovat olleet keskeisessä roolissa jo ennen osoitusvelvollisuuden ottamista osaksi tietosuojalainsäädäntöä, ja nämä oikeudet ovat sisältyneet jo henkilötietodirektiiviin.

[178] Tietosuoja-asetuksen 13 ja 14 artiklat.

[179] Näin esimerkiksi 13(1)(d) edellytetty kuvaus rekisterinpitäjän tai muun tahon oikeutetusta edusta.

[180] WP 260, s. 5-6.

[181] WP 173, s. 14. Läpinäkyvyyttä tarkastellessa tulee huomioida myös esimerkiksi käsittelyn turvallisuuteen liittyvät seikat: näiden liian yksityiskohtainen kuvaaminen saattaisi johtaa käsittelyn turvallisuuden tosiasialliseen heikkenemiseen. Myös liikesalaisuuksien suoja asettaa rajoja läpinäkyvyydelle. Tästä myös WP 248, s. 17.

[182] WP 173, s. 14. Vuosijulkaisuista mainittakoon esimerkkinä tietotilinpäätös, ks. TSV 2017.

osoittamaan ryhtyneensä asianmukaisiin toimiin läpinäkyvyyden varmistamiseksi, saattaa osoitusvelvollisuus näin ollen johtaa myös rekisteröidyn lisääntyneeseen näkyvyyteen henkilötietojen suojan toteutumisesta käsittelytoimissa.

3.3.4. Osoitusvelvollisuus rekisterinpitäjän sisäisenä keinona

Osoitusvelvollisuuden valvontaviranomaiseen ja rekisteröityyn kohdistuvan vaikutuksen lisäksi voidaan kysyä, voiko osoitusvelvollisuus olla merkityksellinen myös rekisterinpitäjän oman toiminnan kannalta, vai onko velvoitteessa kyse vain yhden asetuksen tietosuojavelvoitteista noudattaminen.

Osoitusvelvollisuuden keskeisenä tavoitteena on vakiinnuttaa tietosuoja kiinteäksi osaksi rekisterinpitäjien yrityskulttuuria: tavoitteena on tietosuojan ulottuminen laajasti organisaation jokapäiväiseen toimintaan sen sijaan, että tietosuoja-asiat jäisivät lakiasiainosastoille rasti ruutuun -harjoitteeksi.[183]

Puitteet henkilötietojen suojan toteutumiseksi määräytyvät tietosuojalainsäädännön kautta, joten on perusteltua, että rekisterinpitäjällä on ainakin yleiskäsitys siitä, onko toiminta vaatimustenmukaista. Asetuksessa asetetun henkilötietojen suojan tosiasiallinen käytännön toteutuminen riippuu kuitenkin rekisterinpitäjien toiminnasta: henkilötietojen suoja toteutuu kuitenkin viime kädessä käsittelytoimen yhteydessä.[184] Vaatimustenmukaisuus muodostuu siis rekisterinpitäjän käytännön käsittelytoiminnassa tekemistä ratkaisuista.

Voidaankin kysyä, voidaanko rekisterinpitäjää pitää yhtenä osoitusvelvollisuuden vastaanottajista. Tehtyjen toimenpiteiden kartoittaminen luo osaltaan eittämättä hallinnollista taakkaa.[185] Toisaalta vaatimukset esimerkiksi ylläpitää selostetta käsittelytoimista — sen sijaan, että seloste pitäisi laatia vaikkapa vain viranomaisen niin pyytäessä — kuvastavat lainsäätäjän pyrkimystä kannustaa rekisterinpitäjää suunnitelmalliseen henkilötietojen käsittelyyn. Tulee huomata, ettei osoitusvelvollisuus ole pelkästään näyttövelvollisuus laaditusta dokumentaatiosta. Kuten aiemmin osoitusvelvollisuuden tasojen osalta todettiin, osoitusvelvollisuuden toteuttaminen edellyttää rekisterinpitäjän peilaavan lainsäädännön vaatimuksia omaan toimintaansa ja toteuttavan tarpeelliseksi katsomansa toimet.

[183] WP 168, s. 19.
[184] WP 168, s. 3.
[185] Tästä esim. Bräutigam 2012, s. 421.

Lähtökohtaisesti toimijoiden tulee toki itse tuntea toimintaansa koskevat lainsäädännön vaatimukset — *ignorantia juris non excusat* soveltuu toki tietosuojalainsäädännönkin alalla — mutta käytännössä saattaa muodostua haasteelliseksi varmistaa, että rekisterinpitäjä on huomioinut lainsäädännön velvoitteet ja kykenee varmistumaan niiden noudattamisen toteutumisesta.[186] Vaikuttaisikin siltä, että tietosuojalainsäädännön vaatimukset eivät toistaiseksi ole muodostuneet tehokkaiksi, todellista suojaa antaviksi mekanismeiksi. Yksi syy tähän saattaa olla rekisterinpitäjien puutteellinen ymmärrys tietosuojalainsäädännön vaatimusten osalta. Puutteellinen tietosuojalainsäädännön vaatimusten tunteminen on tullut esille esimerkiksi Suomessa tietosuojavaltuutetun henkilötietolainsäädännön vaatimusten huomiointia verkkopalveluissa koskeneessa selvityksessä.[187] Lainsäädännön vaatimusten tuntemisen lisäksi etenkin suurissa organisaatioissa saattaa olla puutteellinen kokonaiskuva tietojenkäsittelytoimista ja niiden tosiasiallisesta laajuudesta.[188]

Osoitusvelvollisuuden voisi katsoa olevan mekanismi, joka käytännössä pakottaa rekisterinpitäjän tarkastelemaan omaa toimintaansa tietosuojavelvoitteiden valossa. Ideaalitilanteessa tämä itsereflektio toisi rekisterinpitäjälle lisäarvoa tämän arvioidessa toimintaansa sopivia keinoja toteuttaa vaatimustenmukaisuutta sekä johtaisi näin korkeampaan tietosuojaosaamiseen sekä suunnitelmallisuuteen henkilötietojen käsittelyssä. Lisäksi dokumentaation laatiminen ja toimet saattaisivat auttaa esimerkiksi sokeiden pisteiden tunnistamisessa. Toisaalta voidaan kysyä, johtaako dokumentaation laatiminen rekisterinpitäjät tarkastelemaan omaa toimintaa, vai jääkö se pakolliseksi harjoitteeksi, jonka suorittaminen ei johda osaamisen lisääntymiseen tai tehokkaampaan henkilötietojen suojaan.[189] On esitetty, että etenkin toimenpiteiden toimivuuden arvioinnin jättäminen

[186] Lain vaatimusten lisäksi oleellista toki on, että rekisterinpitäjät ymmärtävät, miten velvoitteita tulisi soveltaa käytännön toimintaan. Haasteita saattaa muodostua esimerkiksi lainsäädännön ja oikeuskäytännön tuomista muutoksista sekä lainsäädäntövaatimusten ymmärtämisestä läpi organisaation. Lainsäädännön velvoitteiden noudattamiseen liittyvistä haasteista laajemmin Karhula 2016 s. 68-69.

[187] Selvityksestä ilmeni, että alle puolet tietoturvaloukkauksen tai sen uhan kohteena olleista, selvitykseen vastanneista rekisterinpitäjistä ilmoittivat tuntevansa henkilötietolain vaatimukset tietoturvaedellytysten osalta. Pitkänen — Tiilikka — Warma 2014, s. 9.

[188] Jo pelkästään tarkkarajaisen käsittelytoimen tunnistaminen saattaa olla haastavaa vaikkapa esineiden internetin näkökulmasta, kun tietoa kerätään usein jatkuvastikin lukuisista lähteistä, useiden toimijoiden toimesta ja eri palveluntarjoajien käyttöä varten. De Hert — Papakonstantinou 2016, s. 184.

[189] Koops 2014, s. 225.

pelkästään rekisterinpitäjän itseohjautuvuuden varaan ei välttämättä johda tosiasiallisiin tuloksiin, vaan tehokkuuden arviointi edellyttää ulkoisen tahon osallistumista.[190]

Toistaiseksi osoitusvelvollisuuden on siis katsottu lähinnä lisäävän rekisterinpitäjien hallinnollista taakkaa etenkin pakollisen dokumentaation lisääntyessä. Dokumentaation rooli kuitenkin korostuu osoitusvelvollisuuden käytännön toteuttamisessa. Rekisterinpitäjät tuskin kykenevät varmistamaan käsittelyn vaatimustenmukaisuutta tietämättä itse, miten käsittelytoimet on järjestelty.[191] Etenkin tietosuojaviranomaiset ovat katsoneet osoitusvelvollisuuden edistävän organisaatioiden tietosuojakulttuuria. Jääkin nähtäväksi, voidaanko kulttuuria luoda lainsäädäntötoimilla niin, että osoitusvelvollisuudella tavoitellut edut heijastuisivat myös rekisterinpitäjien käytännön toimintaan.

[190] Bennett 2012, s. 41. Bennett katsoo, ettei pelkkä korkeasta tietosuojan tasosta mahdollisesti saatava markkinaetu välttämättä johda arvioinnin tehokkuuteen, vaan tehokas arviointi saattaisi edellyttää esimerkiksi ulkoisten auditointien käyttöä.
[191] WP kirjelmäliite 17.6.2015, s. 15.

4. Osoitusvelvollisuus EU:n yleisessä tietosuoja-asetuksessa

4.1. Osoitusvelvollisuus henkilötietojen käsittelyä koskevien periaatteiden osalta

4.1.1. Tietosuojaperiaatteet tietosuoja-asetuksessa

Henkilötietojen suojaan liittyvät keskeiset periaatteet ovat vakiintuneet useiden kansainvälisten lainsäädäntöinstrumenttien myötä.[192] Tietosuojaperiaatteilla on tyypillisesti ollut keskeinen rooli tietosuojalainsäädännössä. Roolia voidaan luonnehtia kolmitasoiseksi. Kun periaatteet on otettu osaksi tietosuojalainsäädäntöä, niillä on oma, itsenäinen normatiivinen vaikutus. Toiseksi periaatteilla voi katsoa olevan ohjaava rooli tietosuojalainsäädännön tulkinnassa. Kolmanneksi periaatteilla voidaan myös nähdä olevan suuntaa antava tehtävä uutta tietosuojalainsäädäntöä laatiessa.[193]

Henkilötietodirektiivin tavoin tietosuojaperiaatteet on otettu sellaisenaan osaksi tietosuoja-asetusta, eli niillä on sekä itsenäinen normatiivinen vaikutus että tulkintaa ohjaava vaikutus.[194] Tietosuoja-asetuksen 5 artiklan 1-kohdan mukaan henkilötietojen käsittelyssä tulee noudattaa seuraavia periaatteita:

1) lainmukaisuuden, kohtuullisuuden ja läpinäkyvyyden periaate,
2) käyttötarkoitussidonnaisuuden periaate,
3) tietojen minimoinnin periaate,
4) täsmällisyyden periaate,
5) säilytyksen rajoittamisen periaate, ja
6) eheyden ja luottamuksellisuuden periaate.

Periaatteita koskeva rekisterinpitäjän osoitusvelvollisuus ilmenee 5 artiklan 2-kohdasta: *Rekisterinpitäjä vastaa siitä, ja sen on pystyttävä osoittamaan se, että 1 kohtaa* [tietosuojaperiaatteet] *on noudatettu (”osoitusvelvollisuus”).*

[192] Saarenpää 2012, s. 332.
[193] Bygrave 2014, s. 145.
[194] Tietosuojaperiaatteisiin on viitattu toistuvasti EUT:n ratkaisukäytännössä, ks. esim. C-131/12 Google Spain, kohta 71.

Artikla on kaksitasoinen. Ensinnäkin artiklassa kohdistetaan vastuu tietosuojaperiaatteiden noudattamisesta rekisterinpitäjään. Tämä vastaa sisällöltään henkilötietodirektiivissä kohdistettua vastuuta.[195] Vastuun kohdistuminen rekisterinpitäjään on ilmennyt myös muista henkilötietodirektiivin kohdista.[196] Toiseksi artiklassa säädetään osoitusvelvollisuudesta, joka ilmenee rekisterinpitäjän velvollisuutena *pystyä osoittamaan*, että asetuksen periaatteita on noudatettu. Kuten aiemmin todettua, tätä osoitusvelvollisuutta ei sisältynyt henkilötietodirektiiviin.

Asetuksessa osoitusvelvollisuus on systematisoitu muista periaatteista erilleen, artiklan toiseen kohtaan. Sisällöllisesti osoitusvelvollisuuden voidaankin katsoa toimivan muista periaatteista irrallisella tasolla: muut periaatteet toimivat substanssiulottuvuudella ja luovat toisilleen rajoja, kun taas osoitusvelvollisuus ei muuta muiden periaatteiden sisältöä tai niinkään vaikuta niihin. Osoitusvelvollisuus on vuorovaikutuksessa muiden periaatteiden kanssa vain keinona lisätä periaatteiden tosiasiallista vaikuttavuutta.[197] Voidaankin katsoa, että osoitusvelvollisuus on luonteeltaan funktionaalinen, eikä niinkään sisältöä luova.[198]

Sanamuoto "*pystyttävä osoittamaan, että periaatteita on noudatettu"* viittaa eräänlaiseen rekisterinpitäjän näyttövelvollisuuteen, eli velvollisuuteen näyttää esitetyt tosiasiat — tässä yhteydessä sen, että periaatteet ovat tulleet noudatetuksi — toteen, eikä pelkästään esittää selvitystä siitä, mitä toimia periaatteiden noudattamiseksi on toteutettu. Velvoite vaikuttaisikin ohjaavan rekisterinpitäjän kiinnittämään huomiota myös toimenpiteiden tosiasialliseen tehokkuuteen.

Osoitusvelvollisuus ei kohdistu mihinkään käsittelyn tiettyyn vaiheeseen, vaan ulottuu kaikkeen käsittelyyn. Artiklan sanamuodosta kuitenkin ilmenee sen taaksepäin katsova luonne: rekisterinpitäjän on pystyttävä osoittamaan, että periaatteita *on noudatettu*, eli

---

[195] Henkilötietodirektiivissä periaatteista (direktiivissä "tietojen laatua koskevat periaatteet") säädetään 6 artiklassa, jossa 6(1) luettelee periaatteet ja 6(2) kohdistaa vastuun. Direktiivin sanamuoto poikkeaa hieman asetuksesta: direktiivissä rekisterinpitäjän on *huolehdittava* 1 kohdan noudattamisesta, kun taas asetuksessa rekisterinpitäjä *vastaa* periaatteiden noudattamisesta. Vastaava semanttinen ero esiintyy myös muissa kieliversioissa.

[196] Tämä ilmenee esimerkiksi henkilötietodirektiivin 17 artiklasta, jonka mukaan rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi. Myös aiemmin käsitellyissä OECD:n tietosuojaperiaatteissa kohdistettiin vastuu nimenomaisesti rekisterinpitäjään.

[197] WP 173, s. 5.

[198] Osoitusvelvollisuus ei siis juurikaan määrää, *miten* henkilötietoja tulisi käsitellä. Käytännössä periaatteen toteuttaminen toki edellyttää, että tietoja käsitellään sellaisella tavalla, että voidaan osoittaa periaatteiden tulleen noudatetuksi, eli esimerkiksi sen lisäksi, että kaikelle käsittelylle määritellään käyttötarkoitussidonnaisuuden periaatteen mukainen käsittelytarkoitus eikä henkilötietoa käsitellä "varmuuden vuoksi", rekisterinpitäjä myös dokumentoi määritellyn käsittelytarkoituksen.

osoitusvelvollisuuden osalta osoittamisvastuu kohdistuu jo tapahtuneisiin toimiin. Käytännössä tässä voidaankin katsoa olevan kyse Bennettin osoitusvelvollisuudesta käytäntöjen tasolla (*accountability of practice*), eli jo toteutettujen toimien periaatteidenmukaisuuden dokumentoinnista ja todistamisesta.

4.1.2. Osoitusvelvollisuuden ilmentyminen tietosuojaperiaatteiden kautta

a) Lainmukaisuuden, kohtuullisuuden ja läpinäkyvyyden periaate

Periaate edellyttää, että henkilötietoja tulee käsitellä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi.[199] Näistä asianmukaisuutta ja laillisuutta edellytettiin myös tietosuoja-asetusta edeltäneessä henkilötietodirektiivissä. Lainmukaisuuden edellytyksenä on aina käsittelyn perustuminen vähintään yhteen 6 artiklan käsittelyperusteeseen. Lainmukaisuuden periaatetta ei voikaan tarkastella itsenäisenä periaatteena, vaan se viittaa asetuksen muista velvoitteista ilmeneviin lainmukaisuuden edellytyksiin.[200] Lainmukaisuuden periaate ulottuu osoitusvelvollisuuteen ainakin käsittelyperusteiden kautta: rekisterinpitäjän tulee määritellä kullekin käsittelytoimelle käsittelyperuste, ja osaan perusteista liittyy lisäksi harkinta- tai dokumentointivelvoitteita.[201]

Käsittelyn kohtuullisuutta ei ole määritelty asetuksessa. Asetus antaa kuitenkin painoarvoa rekisteröidyn perustelluille odotuksille etenkin niissä tilanteissa, joissa aiemmin kerättyä tietoa käsitellään uutta tarkoitusta varten.[202] Rekisteröidylle tulee myös kertoa, jos käsittelyyn liittyy erityisiä riskejä.[203] Asianmukaisuutta voitaneen arvioida myös vakiintuneiden käytäntöjen sekä hyvän tietojenkäsittelytavan kautta.[204]

---

[199] Asianmukaisuudesta on käytetty asetuksen englanninkielisessä versiossa termiä "fairness", jonka voidaan katsoa viittaavan reiluun käsittelyyn. Tästä vastaavasti myös henkilötietodirektiivissä Vanto 2003, s. 41; Pitkänen — Tiilikka — Warma 2014, s. 77.

[200] Tästä vastaavasti henkilötietodirektiivissä De Hert ym. 2013, s. 136.

[201] Esimerkiksi rekisteröidyn suostumuksen olemassaolo ja kohde on pystyttävä todentamaan, jos käsittely perustuu suostumukseen (tietosuoja-asetuksen 42 resitaali), ja oikeutettuun etuun perustuva käsittely edellyttää kyseisen edun tunnistamista ja arvopunnintaa (tietosuoja-asetuksen 47 resitaali). Käsittelyperusteisiin liittyvää dokumentaatiota käsitellään tarkemmin osassa 4.3.2.4.

[202] Tietosuoja-asetuksen 50 resitaali. Myöhemmän käsittelyn yhteensopivuudesta laajemmin WP 203, s. 13.

[203] Tietosuoja-asetuksen 39 resitaali.

[204] Esimerkiksi käsitys uudentyyppisten käsittelytoimien tai innovatiivisen teknologian käytön asianmukaisuudesta ei välttämättä ole täysin vakiintunut, joten tällaisen käsittelyn yhdenmukaisuutta tietosuojaperiaatteiden kanssa lienee syytä tarkastella erityisen huolellisesti. Esimerkiksi käsittelytoimiin liittyvää riskiä arvioitaessa otetaan huomioon, onko suunniteltu käsittely luonteeltaan innovatiivista tai uutta tekniikkaa hyödyntävää, ks. tietosuoja-asetuksen 91 resitaali; WP 248, s. 9.

Henkilötietodirektiivissä ei ollut nimenomaista läpinäkyvyyden periaatetta, joskin periaate ilmeni välillisesti esimerkiksi ilmoitusvelvollisuutta ja rekisteröidyn informointia koskevista säännöksistä. Tietosuojauudistuksen yhteydessä kuitenkin katsottiin, etteivät säännökset ole olleet riittävän kattavia tosiasiallisen läpinäkyvyyden toteutumiseksi.[205]

Läpinäkyvyys on yksi keskeisimmistä edellytyksistä sille, että henkilöt voivat varmistaa henkilötietojensa tehokkaan suojan,[206] ja sitä on kuvattu "lainsäädännöllisenä vastauksena perinteiseen toteamukseen siitä, että tieto on valtaa".[207] Kuten aiemmin esitettyä, rekisteröidyn ja rekisterinpitäjän välillä usein vallitsevan tiedollisen epätasapainon aiheuttamat haasteet ovat korostuneet tietojenkäsittelyn muututtua teknologisesti yhä monimutkaisemmaksi.[208] Henkilötietojen käsittely ei useinkaan tapahdu julkisesti: konesaleissa ja teknisissä järjestelmissä tapahtuva käsittely tapahtuu ilman rekisteröityjen läsnäoloa ja joissain tapauksissa ilman, että rekisteröity tosiasiallisesti tietää käsittelyn tapahtumisesta tai sen luonteesta. Käsittelyn tulokset eivät myöskään ole aina, ainakaan välittömästi, rekisteröityjen tiedossa, jotta nämä voisivat reagoida esimerkiksi mahdollisesti henkilötietojensa suojaa loukkaavaksi kokemaansa käsittelyyn.[209] Toisaalta läpinäkyvyyden periaatteiden vastaista olisi myös antaa rekisteröidylle harhaanjohtavaa tietoa käsittelyn luonteesta tai tosiasiallisesta tarkoituksesta.[210]

Keskeisin läpinäkyvyyden ilmenemiskeino on eittämättä rekisteröidylle annettu tieto käsittelystä. Läpinäkyvyyden edellytys heijastuu myös tietosuoja-asetuksen vaatimukseen laatia esimerkiksi tiedonsaantiin, tarkastusoikeuteen ja suostumuksenhallintaan liittyvä viestintä selkeällä ja ymmärrettävällä tavalla. Informoinnin osalta huomiota on kiinnitettävä tiedon ymmärrettävyyteen sekä saatavuuteen, eikä esimerkiksi tietojen pitämisen “jossain” saatavilla ole katsottu riittävän läpinäkyvyyden toteuttamiseksi, vaan tiedot tulisikin asettaa selvästi ja ymmärrettävästi näkyville.[211] Osoitusvelvollisuudella rekisterinpitäjä saattaisikin

[205] KOM (2010) 609, s. 6.
[206] WP 203, s. 13, KOM (2010) 609, s. 6. Myös rekisteröidyn omien tietojen tarkastusoikeutta on pidetty merkityksellisenä, jotta rekisteröity voi varmistua henkilötietojensa käsittelyn paikkansapitävyydestä ja laillisuudesta, ks. esim. C-553/07 Rijkeboer, kohta 49.
[207] Saarenpää 2012, s. 338.
[208] Matzner ym. 2016, s. 218.
[209] De Hert ym. 2013, s. 138. Toisaalta periaatteet sekä rekisteröidyn oikeudet eivät kuitenkaan ole pelkästään loukkauksien varalta muotoiltuja "puolustautumisoikeuksia", vaan tiedonsaannilla ja vaikuttamismahdollisuuksilla on myös itsenäinen arvo, tästä Albers 2014, s. 226.
[210] Bygrave 2014, s. 147.
[211] WP 187, s. 20.

voida osoittaa periaatteen riittävän toteutumisen käytännön käsittelytoiminnassa esimerkiksi osoittamalla viestinnän selkeyttämiseksi tekemiään aktiivisia toimia, kuten esimerkiksi käyttäjätestien käyttöä tietosuojaa koskevien käyttöehtojen kehittämiseksi ymmärrettävämpään suuntaan.[212]

b) *Käyttötarkoitussidonnaisuuden periaate*

Käyttötarkoitussidonnaisuuden periaate on kaksiosainen. Periaatteen mukaan henkilötiedot saa kerätä vain tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä näitä tietoja saa myöhemmin käsitellä alkuperäisen tarkoitusten kanssa yhteensopimattomalla tavalla. Käsittelytarkoitussidonnaisuuden periaatteessa säädetään myös poikkeuksista koskien myöhempää käyttöä yleisen edun mukaisiin arkistotarkoituksiin, tieteellisiin tai historiallisiin tutkimustarkoituksiin sekä tilastollisiin tarkoituksiin liittyen.

Tietyn ja nimenomaisen käyttötarkoituksen edellytyksen voidaan katsoa liittyvän läpinäkyvyyteen, sillä se vähentää väärinymmärryksen mahdollisuutta sekä poikkeavien odotusten riskiä edellyttämällä rekisterinpitäjää määrittelemään käsittelytarkoitus selkeästi silloin, kun tiedot kerätään.[213] Mahdollisen myöhemmän käsittelytarkoituksen yhteensopivuuden arviointi jää osoitusvelvollisuuden myötä rekisterinpitäjän arvioitavaksi ja osoitettavaksi.[214]

Käsittelytarkoituksen määrittely ja kirjaaminen on olennainen osa osoitusvelvollisuuden toteuttamista käyttötarkoitussidonnaisuuden periaatteen noudattamisen osoittamiseksi. Rekisterinpitäjän tulee kyetä määrittelemään käsittelytarkoitus, dokumentoimaan tämä määrittely, sekä pystyä osoittamaan määritelleensä käsittelytarkoituksen. Käsittelytarkoitussidonnaisuutta onkin luonnehdittu "ensimmäiseksi avainaskeleeksi" käsittelyn lainmukaisuuden varmistamiseksi.[215] Käsittelytarkoituksen periaate koskee

---

[212] Vastaavasti rekisterinpitäjällä saattaa olla käytettävissään tietoa siitä, kuinka usein rekisteriseloste tai vastaava tietosuojaseloste on avattu tai luettu. Tietosuojaselosteisiin liittyvistä haasteista on kirjoitettu paljon niin ymmärrettävyyden, laajuuden kuin volyyminkin kannalta. Jo nykypäiväisten käsittelytoimien määrä ja luonne saattaa haastaa läpinäkyvyyden periaatteen toteutumisen, kun tietoa käsittelystä tulisi antaa myös silloin, kun tiedot kerätään esimerkiksi älylaitteen kautta. Rekisteröidyn informointiin liittyvistä haasteista tietosuoja-asetuksessa esim. Bräutigam 2012, s. 427.

[213] WP 203, s.17.

[214] De Hert — Papakonstantinou 2016, s. 186.

[215] WP 203, s. 15 ja 18. Käsittelytarkoitus tulee myös kirjata tietosuoja-asetuksen 30 artiklassa tarkoitettuun selosteeseen käsittelytoimista. Tietosuoja-asetuksen edellyttämää dokumentaatiota käsitellään tarkemmin jaksossa 4.3.

nimenomaan henkilötietojen *keräämistä* ja tätä seuraavaa käsittelyä, joten tarkoitus tulee määritellä viimeistään keräämishetkellä.[216]

c) *Tietojen minimoinnin periaate*

Periaatteen mukaan henkilötietojen on oltava asianmukaisia, olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään. Tarpeellisuusvaatimuksen taustalla on laajoista ja tarpeettomista tietomassojen käsittelystä rekisteröidylle mahdollisesti aiheutuvat riskit, joten periaatetta voikin kuvata "pienimmän mahdollisen puuttumisen" periaatteeksi.[217] Siten esimerkiksi mahdollisesti myöhemmin hyödylliseksi tulevia henkilötietoja ei saa säilyttää tai kerätä "varmuuden vuoksi".[218]

Kuten käyttötarkoitussidonnaisuuden periaatteen osalta, myös minimisointiperiaatteen osalta keskeiseksi osoitusvelvollisuuden kohteeksi nousee asianmukaisen käyttötarkoituksen tunnistaminen kaikelle käsiteltävälle henkilötiedolle, sekä kerättävän ja säilytettävän tiedon tarpeellisuuden analysointi. Uudet henkilötietojen käsittelymuodot, kuten usein ennakoimatonkin massadatan käsittely, saattavatkin aiheuttaa haasteita minimisointiperiaatteen toteutumiselle, kun toisaalta kerättävillä henkilötiedoilla saattaa olla merkittävääkin taloudellista arvoa, eikä kaikkia henkilötietojen käsittelytapoja voida aina määritellä ennalta niin, että voitaisiin perustellusti kertoa, mitä tietoa ei tarvitse enää säilyttää.[219] Osoitusvelvollisuus saattaisikin esimerkiksi edellyttää rekisterinpitäjän punnitsevan ja perustelevan tarpeen käyttää käsittelytoimessa henkilötietoja anonyymien tietojen sijaan.[220]

d) *Täsmällisyyden periaate*

Täsmällisyysperiaatteen mukaan henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettäviä, ja on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot

[216] WP 203, s. 15. Mahdollisen myöhemmän käsittelytarkoituksen yhteensopivuus tulee vastaavasti arvioida ennen tämän myöhemmän käsittelyn aloittamista.
[217] Tästä tarkemmin Saarenpää 2012, s. 335.
[218] WP 223, s. 16. Tästä ilmenee yhteys käyttötarkoitussidonnaisuuden periaatteeseen.
[219] WP 223, s. 16. Esimerkkinä jälkikäteisesti ilmi tulleesta käyttötarkoituksesta voidaan mainita esimerkiksi Googlen influenssaepidemioiden liikkeitä hakusanatrendien perusteella ennustava Google Flu, josta laajemmin Mayer-Schönberger — Cukier 2013, s. 153.
[220] WP 223, s. 16.

poistetaan tai oikaistaan viipymättä. Pyrkimys virheettömyyteen liittyy oikeuteen siitä, että itseään koskevat arvioinnit suoritetaan oikeiden tietojen perusteella.

Osoitusvelvollisuuden kannalta periaatteeseen liittyy haasteita. Virheellisten tietojen käsittely on harvoin rekisterinpitäjänkään etujen mukaista, ja osoitusvelvollisuutta toteuttavat toimenpiteet, jotka varmistaisivat tietojen ajantasaisuuden, merkitsisivät mahdollisesti joissain tapauksissa käsittelyn merkittävää laajentumista. Ottaen huomioon, että henkilötietojen käsittelyä on myös esimerkiksi tietojen säilytys, voidaan kysyä, riittääkö esimerkiksi arkistointitarkoitukseen säilytettävien tietojen osalta niiden ajankohtaisuus ja virheettömyys niiden keräys- tai arkistointihetkellä. Jos käsittelyn tarkoitus on tietojen arkistointi, saattaisi tietojen muu käsittely, kuten päivittäminen ja ajantasaisuudesta huolehtiminen, merkitä käsittelytarkoituksen ylittävää käsittelyä. Tällöin etenkin arkistotietojen kaltaisten staattisten tietojen ajantasaisuudesta varmistuminen saattaisi edellyttää uusien käsittelyvaiheiden lisäämistä ja näin jopa lisätä käsittelyyn kohdistuvaa riskiä.

Toisaalta virheettömyysperiaatetta voidaan tarkastella rekisteröidyn reaktiivisuuden kannalta, jolloin vähimmäisvelvollisuutena rekisterinpitäjän kannalta voisi pitää rekisteröityjen korjauspyyntöjen asianmukaista käsittelyä ainakin staattisen datan osalta. Periaatteen käytännön ulottuvuus saattaa siis vaihdella sen mukaan, onko kyse dynaamisesta ja jatkuvaisluontoisesta vaiko esimerkiksi kertaluontoisesta henkilötietojen käsittelystä.

e) *Säilytyksen rajoittamisen periaate*

Henkilötietojen sallittua säilytysaikaa koskeva säilytyksen rajoittamisen periaate täydentää tietojen laajuutta koskevaa tietojen minimoinnin periaatetta sekä käyttötarkoitusta koskevaa käyttötarkoitussidonnaisuuden periaatetta. Säilytyksen rajoittamisen periaatteen mukaan henkilötietoja saa säilyttää muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. Tämän toteutumisen varmistamiseksi rekisterinpitäjän tulee asettaa määräajat henkilötietojen poistolle tai, jos tarkkojen määräaikojen määrittely ei ole mahdollista, henkilötietojen säilyttämisen tarpeellisuuden määräaikaistarkastelua varten.[221] Tämä ilmenee myös vaatimuksesta laatia seloste käsittelytoimista,[222] johon nimenomaisesti sisältyy rekisterinpitäjän velvollisuus dokumentoida tiedon minimisoinnin periaatteen toteutus säilytysajan osalta.

[221] Tietosuoja-asetuksen resitaali 39.
[222] Tietosuoja-asetuksen 30 artikla.

Tarpeettomia tietoja ei saa siis säilyttää "muodossa, josta rekisteröity on tunnistettavissa": huomautettakoon, että tieto lakkaa olemasta henkilötietoa, kun tunnistettavuus poistetaan. Säilytyksen rajoittamisen periaate ei siis edellytä, että henkilötiedot poistetaan käsittelyn tarpeellisuuden päätyttyä, vaan poistamisen sijaan henkilötiedot voidaan anonymisoida, jolloin anonyymeissä tiedoissa kyse ei ole enää henkilötiedoista.[223] Osoitusvelvollisuuden osalta rekisterinpitäjän tulee toki huomioida asianmukaisen anonymisointitekniikan valintaan liittyvä punninta.

f) Eheyden ja luottamuksellisuuden periaate

Eheyden ja luottamuksellisuuden periaatteen mukaan henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia. Eheyden ja luottamuksellisuuden periaate liittyy kiinteästi henkilötietojen käsittelyä koskeviin tietoturvavaatimuksiin, jotka ilmenevät myös 32 artiklasta.

Kuten edellä esitetystä ilmenee, tietosuoja-asetuksen periaatteet ovat toisiinsa kietoutuneita, ja luonteeltaan osittain päällekkäisiä.[224] Periaatteiden voidaankin kuvata olevan monta ilmentymää yhdestä ja samasta oikeudesta.[225] Periaatteet ovat keskenään samanarvoisia, eikä niitä voida sellaisenaan laittaa tärkeysjärjestykseen. Ei kuitenkaan ole poissuljettua, etteivätkö periaatteet saattaisi olla keskenään ristiriidassa silloin, kun niitä sovelletaan käytännön käsittelytilanteisiin: esimerkiksi säilytyksen rajoittamisen periaate saattaa olla ristiriidassa tietojen eheyden säilyttämisen periaatteen kanssa silloin, jos tietojärjestelmään myöhemmin rakennettu henkilötietojen poisto-ominaisuus johtaa toisiinsa kytköksissä olevien tietojen

[223] Käytännössä tehokkaaseen anonymisointiin liittyy haasteita etenkin silloin, kun kyseessä on laaja tietojoukko. Anonymisointitekniikan valinta sekä tietojen käyttötarkoitus vaikuttavatkin merkittävästi siihen, pystytäänkö tietojoukon käyttöarvo säilyttämään anonymisointitoimenpiteiden jälkeenkin. Anonymisointitekniikoita sekä niihin liittyviä haasteita on käsitelty laajasti tietosuojatyöryhmän mietinnössä WP 216.

[224] Bygrave 2014, s. 145.

[225] Myös julkisasiamies Dámaso Ruiz-Jarabo Colomer tarkasteli - jokseenkin värikkäällä ilmaisulla - tätä sisäistä jännitettä Rijkeboer-tapausta koskenessa ratkaisuehdotuksessaan: *Tässä riita-asiassa ei ole kyse kahdesta eri perusoikeudesta, vaan ikään kuin saman kolikon kahdesta eri puolesta. (...) Tässä tapauksessa on sen sijaan kyseessä yksi ainoa oikeus, jota kalvaa sisäinen ristiriita, jonka sielu on ikään kuin jakautunut Jekyllin ja Hyden tapaan niin, että sen sisällä elää – kuten jatkossa osoitan – sula hyvyys yhdessä kylmän ja laskelmoidun julmuuden kanssa*. C-553/07 Rijkeboer, julkisasiamiehen ratkaisuehdotus, kohta 25.

eheyden rikkoutumiseen. Toisaalta myös käsittelytoimien kehittyminen saattaa jatkossa asettaa haasteita käsittelyperusteiden rajoille.[226]

On ilmeistä, että periaatteet aktualisoituvat eri tavoin eri käsittelytilanteissa. Osoitusvelvollisuuden kannalta periaatteet ilmenevät etenkin asetuksen edellyttämän dokumentaation kautta. Toisaalta yksityiskohtaisempikin punninta ja osoitusvelvollisuuden mukainen dokumentaatio lienee perusteltua etenkin tilanteissa, joissa periaatteet vaikuttaisivat olevan keskenään ristiriidassa. Periaatteiden toteutumisen osoittamisen riittävä taso edellyttäneekin rekisterinpitäjältä tapauskohtaista harkintaa.

4.2. Osoitusvelvollisuus yleisvelvoitteena

4.2.1. Osoitusvelvollisuus 24 artiklan yleisvelvoitteena

Tietosuoja-asetuksen 5 artiklan mukaisen, periaatteisiin kohdistuvan osoitusvelvollisuuden lisäksi osoitusvelvollisuus ilmenee asetuksessa myös 24 artiklan yleisvelvoitteena:

> *1. Ottaen huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tätä asetusta. Näitä toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa.*
>
> *2. Kun se on oikeasuhteista käsittelytoimiin nähden, 1 kohdassa tarkoitettuihin toimenpiteisiin kuuluu, että rekisterinpitäjä panee täytäntöön asianmukaiset tietosuojaa koskevat toimintaperiaatteet.*

Artiklan ensimmäinen kohta on kaksitasoinen. Rekisterinpitäjän tulee toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan *varmistaa*, että käsittelyssä noudatetaan tietosuoja-asetusta. Tässä määriteltyä osoitusvelvollisuutta täydentää asetuksen 74 resitaali, joka edellyttää rekisterinpitäjän voivan osoittaa käsittelytoimien olevan tietosuoja-asetuksen mukaisia, *''toimenpiteiden tehokkuus mukaan luettuna''*. Tämän lisäksi rekisterinpitäjän tulee

[226] Esimerkiksi big datan keskeinen käyttötapa keinona löytää ennakolta tunnistamatonta tietoa ja yhteyksiä laajasta tietojoukosta muodostuu helposti ristiriitaiseksi käsittelyperusteen edellytyksen kanssa. Tästä Barnard-Wills 2017, s. 3.

toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan *osoittaa*, että käsittelyssä noudatetaan tätä asetusta. Asetuksen 24 artiklan jaottelu velvollisuuteen *varmistaa* ja *osoittaa* vastaa siis pääpiirteittäin periaatteita koskevan 5(2) artiklan velvollisuutta *vastata* ja *pystyä osoittamaan* vaatimusten noudattaminen.

Varmistaminen sekä osoittaminen tehdään asetuksen mukaan teknisillä ja organisatorisilla toimilla. 24 artiklassa ei määritellä yksityiskohtaisia keinoja sen toteuttamiseen, vaan rekisterinpitäjälle on jätetty valinnanvapaus parhaaksi katsomiensa keinojen määrittelemiseen ja käyttämiseen. Tämä ilmentää osaltaan aiemmin käsiteltyä lopputulossuuntautuneisuutta, jossa asetuksessa säädetään tietosuojalta lainsäädännössä edellytetystä tasosta, ja jätetään edellytetyn tason toteutuskeinot pääsääntöisesti rekisterinpitäjän harkittaviksi. Osoitusvelvollisuus koskee jokaista käsittelyn vaihetta ja kaikkea tietosuoja-asetuksen piirissä olevaa käsittelyä, joskin yksittäisiin käsittelyn elinkaaren toimiin voi toki heijastua eri vaatimuksia.[227]

Tietosuoja-asetuksen muista artikloista ilmenee joitakin pakollisia toimenpiteitä, jotka osaltaan edistävät osoitusvelvollisuutta. Osoitusvelvollisuuden keinot vaihtelevat käsittelyvaiheen lisäksi esimerkiksi rekisterinpitäjään tai käsittelyn luonteeseen liittyvistä seikoista riippuen. Osoitusvelvollisuuden voidaankin katsoa kohdistuvan sekä lopputulokseen, joka on saavutettava, että toimintamalleihin ja toimenpiteisiin, joita on noudatettava ja suoritettava lopputuloksen saavuttamiseksi.

4.2.2. Osoitusvelvollisuus sisäänrakennetun ja oletusarvoisen tietosuojan tukena

Sisäänrakennetulla ja oletusarvoisella tietosuojalla on kiinteä yhteys osoitusvelvollisuuden totteuttamiselle välttämättömiin teknisiin ja organisatorisiin keinoihin. Tätä korostetaan myös asetuksen 78 resitaalissa:

> *Jotta voidaan osoittaa, että asetusta on noudatettu, rekisterinpitäjän olisi hyväksyttävä sisäisiä menettelyjä ja toteutettava toimenpiteet, jotka vastaavat erityisesti sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita.*

[227] Tietosuojatyöryhmä on sivunnut osoitusvelvollisuuden ajallista ulottuvuutta käsittelyn läpinäkyvyyden kannalta. Läpinäkyvyyden suhteen tämä tarkoittaa esim. käytettävän viestintäkeinon valintaa elinkaaren vaiheen kannalta sopivaksi. WP 260, s. 13.

Sisäänrakennetulla tietosuojalla tarkoitetaan tietosuojaperiaatteiden toteuttamista kaikissa käsittelyn vaiheissa. Periaate on määritelty tietosuoja-asetuksen 25 artiklassa seuraavasti:

> *Ottaen huomioon uusimman tekniikan ja toteuttamiskustannukset sekä käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitukset sekä käsittelyn aiheuttamat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit luonnollisten henkilöiden oikeuksille ja vapauksille rekisterinpitäjän on käsittelytapojen määrittämisen ja itse käsittelyn yhteydessä toteutettava tehokkaasti tietosuojaperiaatteiden, kuten tietojen minimoinnin, täytäntöönpanoa varten asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten tietojen pseudonymisointi ja tarvittavat suojatoimet, jotta ne saataisiin sisällytettyä käsittelyn osaksi ja jotta käsittely vastaisi tämän asetuksen vaatimuksia ja rekisteröityjen oikeuksia suojattaisiin.*

Sisäänrakennetun tietosuojan vaatimus kohdistuu nimenomaisesti rekisterinpitäjään. Rekisterinpitäjä tyypillisesti käyttää käsittelytapoja ja -teknologioita, mutta ei kuitenkaan useinkaan laadi tai suunnittele niitä. Periaate ei siis niinkään aseta vaatimuksia henkilötietojen käsittelyssä käytettyjen ohjelmisto- yms. teknisten ratkaisujen suunnittelijoille tai tarjoajille, vaan rekisterinpitäjälle varsinaisesta käsittelystä vastaavana tahona.[228] Vastuun kohdistumisen taustalla lienee ajatus siitä, että kohdistamalla vastuun rekisterinpitäjään, kannustaa tämä rekisterinpitäjiä valitsemaan sellaisia käsittelyteknologioita, jotka täyttävät lainsäädännön edellytykset.[229]

Säännöksen teksti luo reunaehtoja sisäänrakennetun tietosuojan periaatteelle. Reunaehdot voidaan jakaa kahteen ryhmään, kun toimenpiteiden valinnassa tulee huomioida toisaalta sekä niiden tekniseen ja taloudelliseen toteutettavuuteen liittyviä seikkoja, että käsittelyn luonteeseen liittyviä seikkoja. Vaikka periaate ei sinänsä kohdistu tekniikoiden kehittäjiin, tulee teknisen ja taloudellisen toteutettavuuden edellytystä tarkastella kunkin hetken markkinoiden kontekstissa. Periaate ei edellytä rekisterinpitäjiä toteuttamaan teknisesti tai taloudellisesti kohtuuttomia ratkaisuja, mutta tietosuoja-asetuksen edellytyksiin vastaavien tekniikoiden ja ratkaisujen käytön ja saatavuuden yleistyessä voidaan rekisterinpitäjän katsoa olevan velvoitettu käyttämään käsittelytoimissaan vastaavan tasoisia ratkaisuja tai kehittävän

[228] Tietosuojatyöryhmän aiemmassa kannanotossa tuolloin vielä suunnitteilla ollut sisäänrakennetun tietosuojan periaate katsottiin rekisterinpitäjän vastuun lisäksi kohdennettavaksi myös teknologiasuunnittelijoita ja -tuottajia sitovaksi. WP 168, s. 13.

[229] Hildebrandt — Tielemans 2013, s. 516. Toisaalta sisäänrakennettu tietosuoja voidaan täyttää osin myös sertifikaateilla, jolloin myös sertifikaatin myöntäjän rooli korostuu.

itse omat, paremmat ratkaisut.[230] Viittausta "uusimpaan tekniikkaan" voitaneen pitää lainsäätäjän ratkaisuna sisäänrakennetusti ajantasaisena pysyvän, teknologianeutraalin lainsäädännön tarpeeseen. Sisäänrakennetussa tietosuojassa onkin kyse kontekstuaalisesta ja dynaamisesta velvoitteesta, eli lainsäädännön edellyttämä riittävän tietosuojan taso voi muuttua, jos esimerkiksi käsittely-ympäristössä tapahtuu merkittäviä muutoksia.

Sisäänrakennetulla tietosuojalla on keskeinen yhteys osoitusvelvollisuuden toteuttamiseen. Sisäänrakennetun tietosuojan periaate edellyttää rekisterinpitäjän proaktiivisesti arvioivan suunniteltujen käsittelytoimien vaatimustenmukaisuutta niin käsittelyn alkuvaiheessa kuin kautta käsittelyn elinkaarenkin.[231] Sisäänrakennettuun tietosuojaan kuuluukin sekä vaatimusten implementointi, että vaatimusten toteutumisen seuraaminen.[232] Käytännössä sisäänrakennetun tietosuojan vaatimuksen systemaattinen toteuttaminen on osa sisäistä vaatimustenmukaisuuden arviointia, kun rekisterinpitäjä tunnistaa vaiheet, joissa tietosuojaseikkojen toteutumiseen on syytä kiinnittää huomiota.[233]

Oletusarvoinen tietosuoja koskee tietojen määrän, käsittelyn laajuuden, säilytysajan, sekä tietojen saatavilla olon rajoittamista vain siihen, mikä on kunkin käsittelyn kannalta tarpeen.[234] Oletusarvoinen tietosuoja tukeekin sisällöltään keskeisiä tietosuojaperiaatteita, kuten käyttötarkoitussidonnaisuuden ja tietojen minimoinnin periaatteita. Oletusarvoisen tietosuojan periaatteesta heijastuu aiemmin käsitelty pyrkimys taata korkea tietosuojan taso myös tilanteissa, joissa rekisteröity ei syystä tai toisesta itse aktiivisesti ryhdy toimiin henkilötietojensa suojan turvaamiseksi.

4.3. Osoitusvelvollisuuden toteuttaminen rekisterinpitäjän toiminnassa

4.3.1. Osoitusvelvollisuuden täyttäminen teknisillä ja organisatorisilla toimilla

Tietosuoja-asetuksen rakenteen johdosta osoitusvelvollisuus ilmenee siis kahdesta eri vaatimuksesta, toisaalta periaatteiden osalta, toisaalta yleisvelvoitteena. Systematisointi koskeekin lähinnä sitä, mitä tarkalleen ottaen pitää osoittaa. Vaatimukset ovat kuitenkin yhteen kietoutuneita, ja 5 artiklan henkilötietojen käsittelyperiaatteet heijastuvat läpi asetuksen ja sen

[230] Hildebrandt — Tielemans 2013, s. 517.
[231] Cavoukian - Taylor - Abrams 2010, s. 411.
[232] Cavoukian - Taylor - Abrams 2010, s. 411.
[233] Cavoukian - Taylor - Abrams 2010, s. 413.
[234] Tietosuoja-asetuksen artikla 25(2).

vaatimusten. Käytännön käsittelytoiminnassa toimet, joilla toteutetaan 24 artiklan vaatimusta, toteuttavat usein myös 5 artiklan periaatteita.

Osoitusvelvollisuus on kokonaisvaltainen vaatimus, eikä sitä voida pelkistää yksittäisiin toimenpidevelvoitteisiin. Osoitusvelvollisuuden toteuttaminen edellyttää tapauskohtaista harkintaa, ja sen edellyttämien toimenpiteiden laajuus saattaa vaihdella merkittävästikin käsittelyn luonteesta riippuen.[235] Osoitusvelvollisuutta tuskin voidaan kuitenkaan toteuttaa yhdellä yksittäisellä dokumentilla. Lisäksi samaan käsittelyyn saattaa kohdistua useita dokumentaatio- tai toimenpidevelvoitteita.

Osoitusvelvollisuuden toteuttamiseksi tehtävät toimet voidaan jakaa kahteen ryhmään: tietosuoja-asetuksessa nimenomaisesti edellytettäviin toimenpiteisiin, kuten velvollisuuteen laatia seloste käsittelytoimista, sekä rekisterinpitäjän harkintavallan mukaan käsittelykohtaisesti valittaviin toimiin. Tietosuoja-asetuksen mahdollistama rekisterinpitäjän tilannekohtainen harkintavalta kuvastaakin pyrkimystä toimien skaalautuvuuteen ja tilannekohtaiseen harkintaan. Skaalautuvuus heijastuu myös edellytettävien käytäntöjen laajuudesta. Tietosuojatyöryhmä on osoitusvelvollisuutta käsittelevässä mietinnössään katsonut, että periaatetasolla suurten rekisterinpitäjien voitaisiin katsoa olevan velvoitettuja käyttöönottamaan tiukempia käytäntöjä.[236] Toisaalta rekisterinpitäjän koon lisäksi keskeistä on myös toimintojen laajuus ja niihin liittyvä riski.

Osoitusvelvollisuuden toteuttamiselle ei ole asetuksessa säädetty mitään tiettyjä muotovaatimuksia, vaan rekisterinpitäjä voi siis laatia tarpeelliseksi katsomansa dokumentaation valitsemallaan tavalla. Muotovapaus lienee seurausta pyrkimyksestä skaalautuvuuteen ja joustavuuteen, joskin se saattaa johtaa rekisterinpitäjän kannalta myös epävarmuuteen esimerkiksi arvioitaessa sitä, minkä tasoinen dokumentaatio on riittävä osoitusvelvollisuuden täyttämiseksi.[237] Asetus edellyttää rekisterinpitäjää toimimaan yhteistyössä valvovan viranomaisen kanssa ja esimerkiksi toimittamaan selosteen käsittelytoimista viranomaiselle pyydettäessä, mutta muutoin osoitusvelvollisuuden toteuttamiseen liittyvän dokumentaation esittämisestä tai säilyttämisestä ei säädetä asetuksessa.[238]

---

[235] WP 173, s. 13.
[236] WP 173, s. 13.
[237] WP 173, s. 14.
[238] Tietosuoja-asetuksen resitaali 82.

Yleisvelvoitteen kontekstuaalisuus ja dynaamisuus ilmenee artiklan edellyttämästä toimien ja dokumentaation ajantasaisuudesta. Rekisterinpitäjän tulee tarkistaa ja päivittää toimenpiteet tarvittaessa.[239]

Asetus velvoittaa rekisterinpitäjän ryhtymään tiettyihin, nimenomaisesti määriteltyihin toimenpiteisiin vaatimustenmukaisuuden varmistamiseksi sekä sen osoittamiseksi. Vaikka itse osoitusvelvollisuutta koskevan artiklan yhteyteen ei otettu mukaan tosiasiallisia keinoja toteuttaa osoitusvelvollisuutta, osa muista tietosuoja-asetuksen edellyttämistä toimenpiteistä soveltuu myös osoitusvelvollisuuden toteuttamiseen. Tällaisia velvollisuuksia ovat mm. velvollisuus laatia käsittelytoimintaa kartoittava *seloste käsittelytoimista*, jota edellytetään kaikilta käsittelytoimilta, sekä korkean riskin käsittelyltä edellytettävä *tietosuojan vaikutustenarviointi*. Velvoitteissa korostuu etenkin toiminnan vaatimustenmukaisuuden kartoittaminen ja dokumentointi. Näillä toimilla on kiinteä yhteys osoitusvelvollisuuteen, ja ne soveltuvat laaja-alaisesti erityyppisille käsittelyille.[240]

4.3.2 Tietosuoja-asetuksessa nimenomaisesti edellytetyt toimet

4.3.2.1. Seloste käsittelytoimista

Pakollisen dokumentaation ylläpitämisellä on oleellinen osa osoitusvelvollisuuden noudattamisessa.[241] Tietosuoja-asetuksen 30 artiklan mukaan rekisterinpitäjän on laadittava seloste kaikista vastuullaan olevista käsittelytoimista.[242] Selosteen yhteys osoitusvelvollisuuteen käy suoraan ilmi asetuksen 82 resitaalista: "rekisterinpitäjän tai henkilötietojen käsittelijän olisi ylläpidettävä rekisteriä sen vastuulla olevista käsittelytoimista voidakseen osoittaa, että ne ovat tämän asetuksen mukaisia."[243] Seloste on saatettava valvontaviranomaisen saataville pyydettäessä.[244]

Selosteen vähimmäissisältö määritellään asetuksessa. Osa selosteen sisällöstä koskee käsittelytoimen luonnetta ja sisältöä, kuten tietoa siitä, kenen ja mitä henkilötietoja käsitellään,

[239] Tietosuoja-asetuksen 24 artikla.
[240] VAHTI-ohje s. 21, WP 173, s. 13.
[241] Carey 2015, s. 50
[242] Vaatimus koskee myös henkilötietojen käsittelijää. Käsittelijän velvollisuudet jäävät kuitenkin tutkielman ulkopuolelle. Selostetta käsittelytoimista ei terminologian samankaltaisuudesta huolimatta tule sekoittaa henkilötietolain mukaiseen rekisteriselosteeseen: rekisteriseloste on julkisesti saatavilla pidettävä asiakirja, kun taas seloste käsittelytoimista laaditaan sisäiseen käyttöön.
[243] Selosteesta tietojenkäsittelytoimista osoitusvelvollisuuden toteuttamisen välineenä myös WP 243, s. 18.
[244] Tietosuoja-asetuksen 30(4) artikla.

ja mikä on käsittelyn tarkoitus. Tältä osin seloste käsittelytoimista toimii rekisterinpitäjän käsittelyä koskevan suunnitelmallisuuden osoituksena. Lisäksi selosteessa kuvataan asetuksenmukaisuutta: selosteessa tulee olla "mahdollisuuksien mukaan" sekä kuvaus käsittelyn turvallisuuteen liittyvistä teknisistä ja organisatorisista turvatoimista, että kuvaus henkilötietojen suunnitelluista säilytysajoista. Selosteen minimisisällöstä heijastuukin useita 5 artiklan periaatteita, keskeisimpänä käyttötarkoitussidonnaisuuden periaate käsittelyn tarkoituksen määrittelyn vaatimuksen kautta, säilytyksen rajoittamisen periaate säilytysajan määrittelyn kuvauksen kautta, sekä eheyden ja luottamuksen periaate teknisten ja organisatoristen turvatoimien kuvauksen kautta.

Seloste käsittelytoimista tulee laatia aina tietosuojalainsäädännön piirissä olevan henkilötietojen käsittelyn yhteydessä. Velvoite ei kuitenkaan koske pienimuotoista käsittelytoimintaa harjoittavia rekisterinpitäjiä.[245] Jos rekisterinpitäjänä toimii yritys tai yhdistys jolla on yli 250 työntekijää, tulee seloste laatia riippumatta käsittelyn luonteesta, rekisterinpitäjän toiminnan luonteesta tai laajuudesta, tai mahdollisista käsittelyyn liittyvistä riskeistä.

4.3.2.2. Tietosuojan vaikutustenarviointi korkean riskin käsittelylle

Muuttuneen henkilötietojen käsittelyn toimintaympäristön asettamat vaatimukset ovat johtaneet riskilähtöisyyden korostumiseen tietosuojauudistuksessa. Käsittelytoimien määrän huomattavan kasvun ja käsittelyn arkipäiväistymisen vuoksi on henkilötietojen suojan tehokkaan toteutumisen kannalta entistäkin tärkeämpää, että sääntelyn velvoitteet kohdistuvat etenkin sellaiseen käsittelyyn, joka saattaa johtaa henkilötietojen suojalle aiheutuviin riskeihin. Käytännössä riskilähtöisyys ilmenee etenkin vaatimuksesta laatia tietosuojan vaikutustenarviointi korkean riskin käsittelylle.

Tietosuojan vaikutustenarviointi on yksi tietosuoja-asetuksen uusista vaatimuksista. Vastaavia menettelyjä on ollut käytössä muilla toimialoilla, esimerkiksi ympäristönsuojelussa.[246] Rekisterinpitäjän tulee toteuttaa tietosuojaa koskeva vaikutustenarviointi ennen suunniteltuja käsittelytoimia sellaisille käsittelyille, jotka todennäköisesti aiheuttavat korkean riskin

[245] Tietosuoja-asetuksen 30(5) artiklan mukaan rekisterinpitäjien, joilla on alle 250 työntekijää, ei tarvitse laatia selostetta käsittelytoimista, ellei käsittely ole korkean riskin käsittelyä tai koske arkaluonteisia tietoja tai rikostietoja.

[246] De Hert ym 2013, s. 135. Useat eri eurooppalaiset tietosuojaviranomaiset ovat kannustaneet rekisterinpitäjiä vaikutusarviointien laatimiseen myös ennen tietosuoja-asetuksen voimaantuloa, tästä Carey 2015, s. 297.

luonnollisen henkilön oikeuksille ja vapauksille.[247] Toisin kuin selostetta käsittelytoimista, tietosuojaa koskevaa vaikutustenarviointia edellytetään vain korkean riskin käsittelytoimilta.

Tietosuojaa koskeva vaikutustenarviointi on merkittävä työkalu osoitusvelvollisuuden noudattamiseksi, sillä se toimii osaltaan keinona osoittaa, että rekisterinpitäjä on tarkastellut käsittelyn mahdollisesti aiheuttamia riskejä sekä suunnitellut ja toteuttanut asianmukaisia toimia asetuksen tietosuojavaatimusten noudattamiseksi ja riskien mitigoimiseksi.[248] Arvio pitääkin laatia myös silloin kun ei ole selvää, aiheuttaako käsittely riskejä rekisteröidyn oikeuksille ja vapauksille — myös tässä heijastuu asetuksen riskilähtöisyys.[249]

Poikkeuksena tietosuoja-asetuksessa korostuvasta jälkikäteisen valvonnan lähtökohdasta tietosuojan vaikutustenarviointiin kuuluu tiettyjen edellytysten täyttyessä velvollisuus kuulla tietosuojaviranomaista.[250] Velvollisuus muodostuu silloin, kun rekisterinpitäjä ei kykene toteuttamaan riittäviä toimenpiteitä lieventääkseen vaikutustenarvioinnissa tunnistettuja riskejä hyväksyttävälle tasolle, eli jos vaikutustenarvioinnissa ilmenee korkeita jäännösriskejä. Tällaisesta liian korkeasta jäännösriskistä voi olla kyse esimerkiksi silloin, jos riskin toteutuminen näyttää selvältä, tai jos riskin toteutuminen saattaa johtaa huomattaviin tai peruuttamattomiin seurauksiin rekisteröidyille.[251] Ennakkokuuleminen korvaakin henkilötietodirektiivin mukaisen ilmoitusvelvollisuuden, ja toisaalta siirtää painopistettä kaiken käsittelyn valvonnasta korkean riskin käsittelyn valvontaan. Ennakkokuuleminen puuttuukin rekisterinpitäjän käsittelytoimintaan jossain määrin laajemmin kuin direktiivin mukainen ilmoitusvelvollisuus, sillä vaikutustenarvioinnin kohteena ollutta käsittelyä ei saa aloittaa ennen ennakkokuulemisen valmistumista. Rekisterinpitäjän tulee myös tapauskohtaisesti kuulla rekisteröityjen tai näiden edustajien näkemyksiä käsittelytoimista.[252]

4.3.2.3. Tietosuojavastaavan nimittäminen

Tietosuoja-asetuksessa velvoitetaan rekisterinpitäjä nimittämään tietosuojavastaava tiettyjen edellytysten täyttyessä. Rekisterinpitäjän tulee nimittää tietosuojavastaava aina seuraavissa tilanteissa:

---

[247] Tietosuoja-asetuksen 5 artikla.
[248] WP 248 s. 4.
[249] WP 191, s. 16.
[250] Tietosuoja-asetuksen 36(1) artikla.
[251] WP 248, s. 21-22.
[252] Tietosuoja-asetuksen 35(9) artikla.

a) kun tietojenkäsittelyä suorittaa viranomainen tai julkishallinnon elin (ei kuitenkaan lainkäyttötehtäviä hoitava tuomioistuin),

b) kun rekisterinpitäjän ydintehtävät muodostuvat sellaisista käsittelytoimista, jotka edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa toimien luonteen, laajuuden ja/tai tarkoitusten vuoksi, tai

c) kun rekisterinpitäjän ydintehtävät muodostuvat laajamittaisesta erityisten henkilötietoryhmien (arkaluonteiset henkilötiedot) tai rikostuomioihin liittyvien tietojen käsittelystä.[253]

Velvollisuus nimittää tietosuojavastaava on tässä laajuudessa uusi velvoite, joskin esimerkiksi Saksassa samankaltainen velvollisuus on ollut jo aiemmin.[254] Suomessa velvollisuus on aiemmin ollut tietyillä sosiaali- ja terveydenhuoltoalan toimijoilla.[255]

Tietosuojatyöryhmä on katsonut tietosuojavastaavan olevan "osoitusvelvollisuuden kulmakivi,"[256] mikä ilmenee myös tietosuojavastaavan asetuksessa määritellyistä velvollisuuksista. Tietosuojavastaavan tehtäviin kuuluvat rekisterinpitäjän neuvonta tietosuojavaatimuksiin liittyen ja tietosuojalainsäädännön noudattamisen seuranta ja tähän liittyvät tarkastukset, sekä etenkin vastuunjako, tietosuojatietoisuuden lisääminen, sekä henkilöstön kouluttaminen henkilötietojen suojaan liittyvissä asioissa. Lisäksi tietosuojavastaava neuvoo ja valvoo tietosuojan vaikutustenarviointien laatimisessa sekä toimii yhteyspisteenä valvontaviranomaisille.[257] Asetuksessa korostetaan tietosuojavastaavan velvollisuuksien riskilähtöisyyttä: tietosuojavastaavan on huomioitava tehtäviään suorittaessa käsittelyyn liittyvät riskit etenkin käsittelyn luonteen, laajuuden, asiayhteyden sekä tarkoitusten kannalta.[258]

Nimittämällä tietosuojavastaavan organisaatio ensinnäkin osoittaa, että se on noudattanut asetuksen velvollisuutta nimittää tietosuojavastaava. Osoitusvelvollisuuden kannalta erityisen

[253] Tietosuoja-asetuksen 37 artikla.
[254] Mikkonen 2014, s. 192, WP 243, s. 4.
[255] Tietosuojavastaavan nimittämistä edellytetään näiltä toimijoilta laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) sekä laissa sähköisestä lääkemääräyksestä (61/2007). Lisäksi henkilötietolain 10 §:ssä on edellytetty rekisteriselosteen täyttävää rekisterinpitäjää merkitsemään rekisteriasioista vastaavan henkilön tai rekisterinpitäjän edustajan nimi rekisteriselosteeseen. Tässä on kyse lähinnä yhteyshenkilön ilmoittamisvelvollisuudesta, joten henkilötietolain velvoite on tietosuoja-asetuksen velvoitetta huomattavasti suppeampi.
[256] WP 29 kirjelmäliite 17.6.2015, s. 18.
[257] Tietosuoja-asetuksen 39(1) artikla tietosuojavastaavan vähimmäistehtävistä.
[258] Tietosuoja-asetuksen 39(2) artikla.

merkityksellistä on kuitenkin tietosuojavastaavan tekemä työ tietosuojavelvoitteiden toteutumiseksi. Tietosuojavastaavalla onkin keskeinen rooli osoitusvelvollisuuden täyttämisessä nimenomaan päivittäisten työtehtäviensä kautta: asetuksessa määritellyistä keskeisistä tietosuojavastaavan työtehtävistä tietosuojalainsäädännön noudattamisen seuranta on ensiarvoisen tärkeässä roolissa, jotta rekisterinpitäjällä on ajantasainen ymmärrys siitä, miten tietosuojalainsäädännön vaatimuksia noudatetaan käsittelytoiminnassa.

4.3.2.4. Muu asetuksen edellyttämä dokumentaatio

Edellä käsiteltyjen keskeisten vaatimusten lisäksi asetus edellyttää osoitusvelvollisuutta toteuttavaa dokumentaatiota myös tietyissä, yksityiskohtaisemmissa tilanteissa, kuten käsittelyperusteisiin tai tietosuojaloukkauksiin liittyen.

Oikeutettuun etuun perustuva käsittely

Käsiteltäessä tietoja rekisterinpitäjän tai kolmannen osapuolen oikeutetun edun perusteella on oikeutettuun etuun liittyvä harkinta arvioitava huolellisesti, punniten muun muassa käsittelyn ennakoitavuutta rekisteröidylle.[259] Tietosuojatyöryhmä on henkilötietodirektiivin vastaavaa käsittelyperustetta käsitelleessä muistiossaan katsonut oikeutetun edun käyttöä edeltävän ennakkopunninnan ilmentävän osoitusvelvollisuuden periaatetta, jo ennen osoitusvelvollisuuden tuomista asetuksen tasolle.[260] Tietosuojatyöryhmä katsoi harkinnan dokumentoinnin olevan suositeltavaa osana hyvää tietojenkäsittelytapaa.

Suostumukseen perustuva käsittely

Myös suostumukseen perustuva käsittely johtaa osoitusvelvollisuuteen liittyviin erityisvelvoitteisiin. Rekisterinpitäjän on kyettävä osoittamaan rekisteröidyn antaneen suostumuksensa henkilötietojensa käsittelyyn.[261] Rekisterinpitäjä voi itse valita parhaaksi katsomansa tavan suostumustenhallintaan ja saatujen suostumusten osoittamiseen, huomioiden

---

[259] Tietosuoja-asetuksen 47 resitaali. Tietosuoja-asetuksen 6 artiklassa määritellään tyhjentävästi lailliset perusteet henkilötietojen käsittelylle. Yksi näistä perusteista on oikeutettu etu (Tietosuoja-asetuksen 6(1)(f) artikla). Oikeutettu etu poikkeaa luonteeltaan muista käsittelyperusteista. Oikeutettu etu ei edellytä rekisteröidyn ennakkokontaktia, hyväksyntää tai muuta yhteyttä rekisterinpitäjään, rekisterinpitäjän lakisääteistä roolia tai tehtävää, eikä hengenhätää tai muuta elintärkeään etuun liittyvää kriittistä tilannetta. Kun käsittely tehdään sopimuksen tai suostumuksen perusteella, rekisteröidyllä on ainakin jossain määrin yhteys käsittelyyn, onhan hän solminut sopimuksen tai antanut suostumuksensa. Oikeutettu etu ei sen sijaan edellytä, että rekisteröity olisi ollut yhteydessä rekisterinpitäjään tai muuten osoittanut aktiivisuuttaan: oikeutetun edun perusteella voidaan periaatteessa käsitellä myös sellaisten henkilöiden tietoja, joilla ei ole mitään yhteyttä rekisterinpitäjään, joissain tapauksissa jopa niin, ettei rekisteröidy tule missään vaiheessa tietoiseksi käsittelyn tapahtumisesta (ks. esim. 14 art (5)(b) mahdollistamat poikkeukset rekisteröidyn informointivelvollisuudesta).

[260] WP 217, s.43.

[261] Tietosuoja-asetuksen 7(1) artikla.

kuitenkin sen, ettei suostumustenhallinta itsessään johda liialliseen henkilötietojen käsittelyyn.[262]

Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle

Myös velvollisuudesta ilmoittaa tietoturvaloukkauksesta valvontaviranomaiselle seuraa dokumentointitarpeita. Rekisterinpitäjän tulee kirjata kaikki henkilötietojen tietoturvaloukkaukset, niihin liittyvät seikat, loukkausten vaikutukset sekä toteutetut korjaavat toimet. Dokumentointi laaditaan, jotta viranomaiset voivat varmistua loukkausta koskevan artiklan noudattamisesta.[263]

4.3.3. Keskeisiä rekisterinpitäjän valittavissa olevia keinoja osoitusvelvollisuuden toteuttamiseksi

Käsittelytoimien moninaisuuden vuoksi useat osoitusvelvollisuuden toteuttamiseksi tehtävät toimet edellyttävät tapauskohtaisuutta, eivätkä ne välttämättä sovi mielekkäästi toteutettavaksi toisistaan poikkeaviin käsittelytoimiin. Tietosuojatyöryhmä on huomauttanut, että "yksi koko sopii kaikille" -lähestymistapa saattaisikin johtaa siihen, että toteutettavat toimet eivät olisi tarkoituksenmukaisia ja siten epäonnistuisivat.[264]

Osoitusvelvollisuuden vapaamuotoisuus mahdollistaa tietosuojan toteuttamiseksi tehtyjen toimenpiteiden valitsemisen kunkin käsittelytoimen tarpeiden mukaan. Osoitusvelvollisuuden roolissa tietosuojan kehittämisessä "teoriasta käytäntöön" on kiinnitetty erityistä huomiota skaalautuvuuteen.[265] Sopivan keinon valinnassa tietosuojatyöryhmä on nostanut esille kaksi henkilötietodirektiivissäkin mainittua elementtiä: käsiteltävien tietojen luonne sekä käsittelyyn liittyvät riskit.[266]

Osoitusvelvollisuuden mahdollisia toteutuskeinoja on tutkittu myös OECD:n tietosuojasuosituksen sekä Accountability projects -työryhmien yhteydessä. Aiemmin käsitelty OECD:n tietosuojasuositus päivitettiin 2013 vastaamaan teknologisen kehityksen sekä

[262] WP 259, s. 20.
[263] Tietosuoja-asetuksen 33(5) artikla.
[264] WP 173, s. 13.
[265] WP 173, s. 3.
[266] WP 173 s. 13, tästä henkilötietodirektiivin 17 artikla: *ottaen huomioon kehityksen taso ja toimenpiteiden kustannukset on taattava asianmukainen turvallisuuden taso suhteessa käsittelyn riskeihin ja suojattavien tietojen luonteeseen.* Toisaalta tätä käsitteellistä jakoa voinee kritisoida, sillä ulottuvuudet eivät ole täysin itsenäisiä, vaan käsiteltävien tietojen luonne muodostaa yhden osan käsittelyyn liittyvistä riskeistä.

henkilötietojen merkityksen korostumisen aiheuttamiin tarpeisiin.[267] Tässä päivitetyissä suosituksissa osoitusvelvollisuutta koskevaa kohtaa on täydennetty uudella kohdalla, jossa esitetään rekisterinpitäjän vastuullisen tietosuojaohjelman piirteitä. Suositus korostaa käsittelyn rakenteen, mittakaavan, sekä käsittelytoimien mahdollisen arkaluontoisuuden huomioimista rekisterinpitäjän valitessa asianmukaisia toteutuskeinoja vaatimuksenmukaisuuden noudattamiseksi. Lisäksi huomiota kiinnitettiin jatkuvaan tietosuojakulttuuriin: tietosuojan tulisi OECD:n suositusten mukaan olla sisäänrakennettuna rekisterinpitäjän hallintorakenteisiin, ja toimenpiteitä tulisi päivittää tarpeen mukaan, ja niiden toteutumista tulisi valvoa myös sisäisesti. Yleisen vaatimustenmukaisuuden lisäksi korostettiin valmiutta vastata tietosuojapoikkeamiin.

Vaikka osoitusvelvollisuus itsessään onkin tietosuoja-asetuksen myötä uusi velvoite, käytännön toimintatavat osoitusvelvollisuuden toteuttamiseksi eivät ole täysin uusia, vaan osa tietosuojatyöryhmän ja vastaavien tahojen esittelemistä toimenpiteistä — kuten esimerkiksi organisaation tietosuojaperiaatteiden laatiminen — ovat jo nyt tyypillisesti käytössä olevia parhaita käytäntöjä etenkin dataintensiivisillä aloilla.[268] Vastaavanlaisia, lainsäädännön vaatimusten organisaation toiminnan osaksi tuovia toimenpiteitä on liike-elämässä tyypillisesti käytössä myös compliance- eli vaatimustenmukaisuusohjelmien yhteydessä, ja tietosuoja otetaankin nykyään usein osaksi yrityksen compliance-ohjelmaa.[269]

Organisaation sitoutuminen osoitusvelvollisuuteen ja ulkoisia vaatimuksia vastaavien sisäisten käytäntöjen käyttöönotto

Ulkoisten vaatimusten tarkastelu ja tuominen rekisterinpitäjän toimintaan vastaa aiemmin käsiteltyä Bennettin osoitusvelvollisuutta periaatteiden ja menettelyjen tasolla: rekisterinpitäjä määrittele asianmukaiset ja käsittelytoiminnalle sopivat toimenpiteet ja ottaa ne käytäntöön.

Sisäisten käytäntöjen määrittelyn keinona voidaan hyödyntää esimerkiksi organisaation tietojohtamista ohjaavien, kirjallisten ja sitovien tietosuojaperiaatteiden laatimista[270] tai tietosuojan nykytila-analyysia, jolla voidaan verrata käsittelytoimien ja

[267] TATTI-mietintö s. 98.
[268] Mikkonen 2014, s. 192-193.
[269] Tietosuojan merkitys compliance-ohjelmien osa-alueena on korostunut etenkin tietosuoja-asetuksen soveltamisen alkamisen lähestyessä. Ratsula 2016, s. 131.
[270] WP 173, s. 12.

tietosuojakyvykkyyksien nykytilaa tietosuoja-asetuksen vaatimuksiin, jotta voidaan tunnistaa puutteet ja kehityskohteet sekä suunnitella tarpeelliset toimenpiteet.[271]

Sisäiset käytännöt on perusteltua määritellä jo ennen uusien käsittelytoimien aloittamista.[272] Vaatimustenmukaisuudenhallinnan tuominen jo käsittelyn alkuvaiheeseen on olennainen osa myös aiemmin käsiteltyä sisäänrakennettua tietosuojaa. Lisäksi organisaation sitoutumisessa korostuu "tietosuojakulttuurin" merkitys.[273]

Keinot toteuttaa tietosuojaperiaatteita, kuten työkalut ja koulutus

Työkaluista mainittakoon rekisterinpitäjän toimintaa tukeva dokumentaatio sen ymmärtämiseksi, miten käsittelytoimet on järjestelty ja miten niitä toteutetaan.[274] Aiemmin mainitun selosteen käsittelytoimista lisäksi käsittelyn suunnitelmallisuutta ja tarkoituksenmukaisuutta voidaan tarkastella myös henkilötietojen käsittelyyn liittyvillä kartoituksilla ja käsittelytoimien inventaarioilla.[275]

Tietosuojavastaavan sekä muiden tietosuojasta vastaavien työntekijöiden nimittämisen ohella tietosuojatyöryhmä korostaa tietosuojaosaamisen merkitystä läpi organisaation: riittävä koulutus on keskeistä etenkin henkilötietoja käsitteleville sekä niistä vastaaville henkilöille, kuten tietohallintopäälliköille, tietotekniikan kehittäjille sekä johtajille.[276] Toisaalta tulee huomata, että toimialasta riippuen merkittäväkin osa yrityksen työntekijöistä saattaa käsitellä henkilötietoja, ja käsittelytavat saattavat poiketa merkittävästi työtehtävistä riippuen. Tällöin lienee oleellista noudattaa riskiperusteista lähestymistapaa ja tunnistaa työntekijät, jotka toimivat rooleissa, joissa käsitellään laajoja määriä henkilötietoja, tai joissa käsittely voi esimerkiksi tietojen luonteesta johtuen johtaa tietosuojariskeihin.

Järjestelmällinen sisäinen valvonta ja ulkoiset tarkastukset

Osoitusvelvollisuus edellyttää toteutettujen toimien tehokkuuden osoittamista. Toimenpiteiden tosiasiallisen toteutumisen varmistamisessa ja käytännön seurannassa voidaan käyttää esimerkiksi sisäisiä ja ulkoisia auditointeja.[277] Jotta sisäisesti määriteltyjen toimintatapojen

[271] VAHTI-ohje, s. 31.
[272] WP 173, s. 12.
[273] WP 173, s. 9. Tietosuojatyöryhmä tuo esille myös tietosuojan hallintaan osoitettavien resurssien riittävyyden.
[274] WP kirjelmäliite 17.6.2015, s.15.
[275] WP 173, s. 12.
[276] WP 173, s. 12.
[277] WP 173, s.12.

noudattamisesta voidaan varmistua, saattaa myös olla perusteltua laatia menettelyt tilanteisiin, joissa on toimittu sisäisten ohjeiden vastaisesti.[278] Kyseeseen saattaa tulla myös kanavat, joiden kautta väärinkäytöksistä ja muusta mahdollisesti lainsäädännön velvoitteiden vastaisesta toiminnasta voidaan ilmoittaa. Merkittävistä tietosuojaloukkauksista seuraa jo sellaisenaan asetuksen mukainen ilmoitusvelvollisuus viranomaisille, mutta rekisterinpitäjän on toki perusteltua tietää myös riskeistä ja poikkeamista vaikka ne eivät ylittäisikään rekisterinpitäjän ilmoitusvelvollisuutta. Tulee myös huomata, että ilmoitusvelvollisuuden toteuttaminen edellyttää rekisterinpitäjältä kyvykkyyttä sekä havaita poikkeamat että selvittää niiden mahdolliset seuraamukset.[279] Myös etenkin käsittelytoimien lokitus saattaa tyypillisesti olla tarpeen käsittelyn valvonnaksi ja seuraamiseksi esimerkiksi mahdollisten väärinkäytösten selvittämiseksi.[280]

Sertifikaatit ja itsesääntely

Asetus mainitsee myös sertifiointimekanismit sekä tietosuojasinetit ja -merkit, joiden avulla rekisteröity voisi nopeasti arvioida palveluntarjoajan todellisen tietosuojan tason.[281] Asetus viittaa viranomaisten laatimaan ja hallinnoimaan sertikaattimalliin, eikä niinkään markkinoilla esiintyviin sertifikaatteihin. Tällä hetkellä näitä sertifikaatteja ei ole vielä kehitetty. Tietosuojatyöryhmä kuitenkin katsoi osoitusvelvollisuuden ottamisen osaksi lainsäädäntöä mahdollisesti myös edistävän sertifiointimekanismien kehittymistä.[282] Rekisterinpitäjät voivat toki ottaa käyttöönsä myös muita kuin viranomaisten hallinnoimia sertifikaatteja. Yleisesti käytössä olevista, asetuksen velvoitteita koskevista sertifikaateista keskeisin lienee informaatioteknologiaa koskeva SFS-ISO/IEC 27000-standardi.[283]

Läpinäkyvyys ja keinot yksilön osallistumiseen

Kuten aiemmin mainittua, läpinäkyvyys on kiinteässä yhteydessä osoitusvelvollisuuden toteuttamiseen ja tavoitteisiin. Tietosuoja-asetuksen vähimmäisvaatimus läpinäkyvyyden toteuttamiselle on asetuksessa edellytetty rekisteröidyn asianmukainen tiedottaminen.[284]

---

[278] Compliance-näkökulmasta Ratsula 2016, s. 209.
[279] VAHTI-ohje, s. 26.
[280] VAHTI-ohje s. 25.
[281] Tietosuoja-asetuksen 42 ja 43 artiklat sekä 100 resitaali.
[282] WP 173, s. 17. Asetuksen sertifikaattimallista laajemmin De Hert — Papakonstantinou 2016 s. 191-192.
[283] Standardista laajemmin https://www.iso.org/isoiec-27001-information-security.html. [Tieto haettu 1.1.2018].
[284] Tietosuoja-asetuksen 12-14 artiklat. Todettakoon, että asetus edellyttää, että käsittelystä annetaan tietoa rekisteröidylle, eli mitään yleistä informointivelvollisuutta laajemmalle yleisölle tai muille tahoille kuin rekisteröidylle ei sinänsä ole. Tämä poikkeaa henkilötietolain velvollisuudesta laatia rekisteriseloste ja pitää se yleisön saatavilla. Asetuksen 58 resitaalissa kuitenkin suositellaan antamaan tietoja yleisölle esimerkiksi internetsivuston kautta.

Läpinäkyvyyden keinona mainittakoon tietotilinpäätös. Tietosuojavaltuutettu laatinut jo 2012 ohjeen tietotilinpäätöksen julkaisusta. Myös tässä, ennen tietosuoja-asetuksen lopullisen tekstin muotoutumista laaditussa ohjeessa on mainittu tietotilinpäätös yhtenä osoitusvelvollisuuden mukaisena menettelytapana.[285] Tietotilinpäätöksen on katsottu lisäävän myös henkilötietojen käsittelyn suunnitelmallisuutta: se ohjaa tarkastelemaan käsittelyä systemaattisesti ja kriittisesti. Tietotilinpäätös voidaan kohdistaa joko organisaation sisäiseen tietojohtamiseen tai raporttina organisaation sidosryhmille.[286]

4.4. Osoitusvelvollisuuteen liittyviä haasteita rekisterinpitäjille

Tietosuoja-asetuksen soveltaminen alkaa 25.5.2018, ja tätä kirjoittaessa valmistautuminen asetuksen tuomiin muutoksiin on käynnissä. Valmistautuminen aiheuttaa merkittäviä kustannuksia rekisterinpitäjille, ja aiemman lainsäädännön mukaisten käsittelyjärjestelmien käytön jatkaminen tietosuoja-asetuksen tultua sovellettavaksi saattaa edellyttää merkittäviäkin jälkikäteisiä muutoksia tietojärjestelmiin.[287]

Osoitusvelvollisuuden käytännön toteuttamiskeinojen tulkinnanvaraisuus mahdollistaa tilannekohtaisen joustavuuden sekä skaalautuvien ratkaisujen toteuttamisen. Tulkinnanvaraisuus johtaa kuitenkin myös epävarmuuteen edellytettävien toimenpiteiden luonteesta ja riittävyydestä.[288]

Esimerkiksi edellä käsitellyt, tietosuojatyöryhmän osoitusvelvollisuutta koskeneessa mietinnössä esitellyt osoitusvelvollisuuden keinot ovat jo nyt tyypillisiä tietosuojahallintoon liittyviä keinoja: ohjeistuksen on kuitenkin katsottu keskittyvän esittelemään velvoitetta

[285] Tietosuojavaltuutettu on laatinut oppaan tietotilinpäätöksen laatimisesta, http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfpzNVCh/Laadi_tietotilinpaatos.pdf [tieto haettu 1.1.2018].

[286] Suomessa muutamat organisaatiot ovat viime vuosina laatineet julkisia tietotilinpäätöksiä. Näistä mainittakoon Liikenteen turvallisuusvirasto (Trafi 2017), Viestintävirasto (Viestintävirasto 2016), sekä Väestörekisterikeskus (tiivistelmä, Väestörekisterikeskus 2016). Esimerkiksi Trafi mainitsee pyrkineensä organisaation tiedon tilan tarkasteluun keinona toteuttaa tietostrategiaa. Lisäksi julkaisussa korostetaan luottamuksen merkitystä etenkin toimintaympäristössä, jossa tiedon merkitys ja hyödynnettävyys on kasvanut merkittävästi. Trafi 2017, s. 5.

[287] Järjestelmien jälkikäteinen muuttaminen tietosuojavaatimusten mukaiseksi saattaa aiheuttaa merkittäviäkin kustannuksia, tästä Saarenpää 2008, s. 140-141. Haasteita voi aiheuttaa myös puutteet, joiden korjaaminen jälkikäteen saattaa olla mahdotonta: jos tiedosta ei ole kerätty metatietoja, kuten tallennusaikaa tai muuta aikaleimaa, saattaa tiedon säilytysajan arviointi olla haastavaa.

[288] WP 173, s. 14.

"periaatteiden ja konseptien kielellä"[289], eikä ohjeistus ota kantaa esimerkiksi siihen, miten osoitusvelvollisuuden toteuttamiseksi tehtyjen keinojen riittävyys arvioidaan.

Yksi ratkaisu tulkinnanvaraisuuteen voi olla viranomaisten antama tarkentava ohjaus. Esimerkiksi tietosuojatyöryhmä on osoitusvelvollisuutta koskevassa mietinnössään katsonut, että viranomaisten antama ohjaus voi toimia tukena tietosuoja-asetuksen vaatimusten käytännön toteuttamiselle.[290] Euroopassa tietosuojatyöryhmän lisäksi suosituksia on tietosuojan alalla antanut myös Euroopan neuvosto.[291]

Tietosuoja-asetuksen osalta tietosuojaviranomaisten ohjauskäytännöissä on ollut merkittävää maakohtaista vaihtelua. Osassa jäsenvaltioita tietosuojaviranomaiset ovat antaneet laajaltikin asetuksen noudattamiseen ohjeistusta[292] tai päivittäneet olemassa olevaa ohjeistustaan asetuksen vaatimuksia vastaavaksi[293]. Toisaalta esimerkiksi Suomessa tietosuojavaltuutettu ei ole laatinut erillistä ohjeistusta asetukseen valmistautuville tahoille, vaan kehottanut rekisterinpitäjiä tutustumaan tietosuojatyöryhmän laatimiin ohjeistuksiin.[294]

Myös hitaus liittyen kansallisen harkintavallan käyttöön mahdollisen täydentävän kansallisen lainsäädännön laadinnassa saattaa lisätä epävarmuutta rekisterinpitäjien tietosuoja-asetuksenmukaisuuteen liittyvissä valmistelutoimissa. Esimerkiksi lasten henkilötietojen käsittelyä koskevasta ikärajasta voidaan säätää kansallisella lailla, mutta osassa maissa tarkka ikäraja ei ole vielä selvinnyt, ja esimerkiksi Suomessa tarkka ikäraja selvinnee vasta joitain kuukausia ennen asetuksen sovellettavaksi tuloa.[295]

---

[289] Alhadeff — Van Alsenoy — Dumortier 2012 s. 26.

[290] WP 173, s. 14. Tästä mainittakoon esimerkkinä esimerkiksi Kanadan tietosuojaviranomaisen (Office of the Privacy Commissioner of Canada) PIPEDA-itsearviointityökalu.

[291] Saarenpää 2012, s. 324.

[292] Esimerkiksi Italian tietosuojaviranomainen Garante on julkaissut vuoden 2017 aikana useita ohjeistuksia liittyen mm. suostumukseen, oikeutetun edun määrittelyyn, rekisteröidyn informointiin, rekisteröidyn oikeuksiin, sekä henkilötietojen kolmansiin maihin siirtoihin liittyen. Myös osoitusvelvollisuudesta ja riskilähtöisestä lähestymisestä on annettu ohjeistusta. Ohjeistukset ovat saatavilla viranomaisen verkkosivuilla, ks. Garante 2017.

[293] Esimerkiksi Ison-Britannian ICO kuvaa verkkosivuillaan päivittäneensä jo olemassaolevia ohjeita koskien etenkin aihealueita, joiden soveltamisesta tietosuoja-asetuksen myötä tietosuojatyöryhmä on antanut lausuntoja, ks ICO 2017b.

[294] Tietosuojavaltuutettu toteaakin tarjonneensa "eioota" lukuisiin, määrältään lisääntyviin yhteydenottoihin ja tiedusteluihin tietosuoja-asetuksen tulkinnasta, ks. Aarnio 2017.

[295] EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmä on päätynyt ehdottamaan, että kansallista liikkumavaraa tullaan käyttämään, mutta ikärajasta ei ole tehty päätöstä. Mietinnössä lähtökohtana on joko 13 tai 15 vuoden ikäraja. TATTI-mietintö, s. 50. Komission Better Internet for Kids -sivustolla seurataan kansallisen liikkumavaran käyttöä ikärajan osalta. Seurannan perusteella useassa jäsenvaltiossa ikäraja on vahvistettu kesällä 2017, vajaa vuosi ennen tietosuoja-asetuksen sovellettavaksi tulemista.

Yksi tietosuoja-asetuksen keskeisimpiä muutoksia on viranomaisen mahdollisuus määrätä hallinnollisia sanktioita. Huomattavan korkea enimmäissanktiotaso poikkeaa merkittävästi henkilötietodirektiivin aikaisista, tietosuojaloukkauksiin kohdistuneista taloudellisista riskeistä.[296] Sanktiouhalla lienee eittämättä vaikutus yritysten halukkuuteen noudattaa asetuksen vaatimuksia. Toisaalta sanktionuhka korostaa jo valmiiksi epävarman oikeustilan haasteellisuutta.[297] Kun asetus on laadittu verrattain avoimella kielellä, eikä tarkkaa viranomaisohjeistusta ole saatavilla, jää riittävän osoitusvelvollisuuden toteuttamisen taso korostetusti rekisterinpitäjän harkittavaksi ainakin siihen saakka, kunnes velvoitteeseen liittyvät käytännöt vakiintuvat ja odotettava taso selkeytyy mahdollisten sisältövaatimusten tarkentuessa. Velvoitteen skaalautuvuuden vuoksi lienee kuitenkin ilmeistä, että rekisterinpitäjälle jää jossain määrin harkintavaltaa osoitusvelvollisuuden käytännön toteuttamisessa. Sama dokumentaatio ja samat toimenpiteet tuskin soveltuvat jatkossakaan kaikille käsittelytoimille.

Sisämarkkinatavoitteen toteutumisen osalta sääntelyn ylätasoisuus sekä sanktioriski saattaa johtaa rekisterinpitäjien "ylivarovaisuuteen", jos rekisterinpitäjät jättävät hyödyntämättä lainsäädännön mahdollistamat käyttäytymismahdollisuudet oikeustilan epävarmuuden vuoksi.[298]

Osoitusvelvollisuuden toteuttamisen kannalta haasteelliseksi voi nousta myös vaatimustenmukaisuuden dynaamisuus: muuttuvan informaatioympäristön ja teknologian kehityksen myötä tällä hetkellä tietosuojalainsäädännön vaatimukset täyttävä toiminta saattaa muodostua jatkossa riittämättömäksi, jos esimerkiksi käytettävissä oleva teknologia muuttuu merkittävästi.

https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=2019355 [tieto haettu 1.1.2018].

[296] Eräissä jäsenmaissa, kuten esimerkiksi Iso-Britanniassa, valvontaviranomainen on voinut määrätä jo henkilötietodirektiivin aikana sanktiomaksuja, joskin niiden enimmäistaso on ollut huomattavasti tietosuoja-asetuksen mahdollistamaa enimmäistasoa matalampi.

[297] VN 2017, s. 10.

[298] Keinänen 2016, s. 78.

5. Lopuksi

Henkilötietojen käsittelyssä on tultu teknologiseen murroskohtaan, jossa informaatioyhteiskuntaa edeltänyt lainsäädäntö ei ole enää täysin kyennyt vastaamaan niihin haasteisiin, joita uusista henkilötietojen käsittelymuodoista on seurannut. EU:n pitkään valmistellussa tietosuojauudistuksessa pyrittiinkin vastaamaan muuttuvan toimintaympäristön tietosuojalainsäädännölle asettamiin edellytyksiin. Asetusuudistuksen tavoitteena oli sääntelyn ajantasaistaminen ja teknologian kehitykseen vastaaminen, mutta myös sisämarkkinaulottuvuuden vahvistaminen lainsäädännön harmonisoinnilla.

Digitaalisten sisämarkkinoiden tehokkaan toiminnan vuoksi on oleellista, että lainsäädännöllä kyetään varmistamaan henkilötietojen suoja myös sellaisen teknologioiden ja käsittelymuotojen osalta, jotka eivät vielä tässä vaiheessa ole yleisesti käytössä tai joita ei vielä ole keksittykään. Nämä tavoitteet tehokkaammalle ja laajoihin käsittelymuotoihin soveltuvalle suojakeinolle ilmenevätkin osoitusvelvollisuudesta — velvoite on yleiselle tasolle kirjoitettu eikä sido rekisterinpitäjää mihinkään tiettyyn tekniseen toteutustapaan.

Rekisterinpitäjät käsittelevät yhä enemmän henkilötietoja, ja kehittyvän teknologian mahdollistama käsittely on yhä monimutkaisempaa. Toisaalta rekisterinpitäjä on usein se taho, joka hyötyy eniten käsittelystä ja tuntee parhaiten suorittamansa käsittelytoimet ja -tavat sekä mahdollisesti myös niihin sopivat suojakeinot. Osoitusvelvollisuudella onkin pyritty ohjaamaan rekisterinpitäjiä sisäiseen oman toimintansa tarkasteluun, jotta rekisterinpitäjä voi kyetä osoittamaan sen, mitkä toimet se on katsonut tarpeellisiksi tietosuoja-asetuksen velvoitteiden noudattamiseksi. Osoitusvelvollisuuden myötä vastuu henkilötietojen käsittelyn lainmukaisuudesta ja henkilötietojen suojan toteuttamisesta siirtyykin entistä enemmän juuri rekisterinpitäjille.

Henkilötietojen suojan tehokkaaseen ja tosiasialliseen toteutumiseen vaikuttaa olennaisesti se, miten rekisterinpitäjäorganisaatioissa suhtaudutaan tietosuojakysymyksiin. Tietosuojatyöryhmän pyrkimys saada tietosuoja osaksi yritysten toimintakulttuuria onkin perusteltu: lainsäädännölliset toimet saattavat jäädä riittämättömiksi, jos käytännön käsittelytoiminnassa tietosuojaseikat jäävät toissijaisiksi.

Osoitusvelvollisuus on yleisluontoinen velvoite, eikä sitä koskevien artiklojen yhteydessä päädytty säätämään tarkoista keinoista, joilla rekisterinpitäjät voivat täyttää velvoitteen.

Osoitusvelvollisuus koskeekin nimenomaan lopputulosta, joka rekisterinpitäjien tulee toiminnassaan saavuttaa, ja siitä on pyritty luomaan eri käsittelymuotoihin mukautuva velvoite. Toimenpiteet, jotka organisaatio valitsee tietosuojan tasosta huolehtimiseksi, voidaan dokumentoida osana osoitusvelvollisuutta ja näin mahdollisesti kannustaa rekisterinpitäjiä ryhtymään asianmukaisiksi katsomiinsa toimiin henkilötietojen suojan toteuttamiseksi. Uutena velvoitteena osoitusvelvollisuudella ei kuitenkaan ole vielä vakiintunutta sisältöä, ja sen määritelmä on jäänyt myös asetuksen tasolla tulkinnanvaraiseksi. Osoitusvelvollisuuden täsmentyminen onkin jätetty viranomaisten mahdollisten tulevien tulkintasuositusten sekä myöhemmän oikeuskäytännön varaan.

Tietosuoja-asetus asettaa kuitenkin myös nimenomaisia edellytyksiä käsittelytoimien vaatimustenmukaisuuden tarkasteluksi. Nämä tietosuoja-asetuksen nimenomaiset edellytykset, kuten tietosuojan vaikutustenarviointi sekä edellytys vaatia seloste käsittelytoimista toimivatkin käytännössä myös keskeisinä osoitusvelvollisuuden noudattamiskeinoina. Dokumentointivelvoitteilla pyritään ohjaamaan rekisterinpitäjää itse tarkastelemaan toimintansa vaatimustenmukaisuutta — toisaalta jää nähtäväksi, muodostuvatko lukuisat velvoitteet lähinnä hallinnolliseksi taakaksi, vai lisääkö niiden laatiminen tosiasiassa rekisterinpitäjän ymmärrystä oman toimintansa luonteesta ja vaatimustenmukaisuudesta. Velvoitteista heijastuu myös pyrkimys tietosuojakulttuurin luomiseen, ja esimerkiksi nimenomainen edellytys nimittää tietosuojavastaava johtanee parhaimmillaan jopa tietosuojan merkityksen korostumiseen organisaatiossa.

Tietosuoja-asetusta aletaan soveltaa toukokuussa 2018, ja tätä kirjoittaessa rekisterinpitäjien valmistautumistyö asetuksen tuomiin vaatimuksiin on käynnissä. Asetuksen tullessa sovellettavaksi osoitusvelvollisuus tulee ensimmäistä kertaa osaksi eurooppalaista tietosuojalainsäädäntöä, ja lainsäätäjä on pyrkinyt vastaamaan käsittely-ympäristön henkilötietojen suojalle aiheuttamiin haasteisiin tuomalla lainsäädännön tasolle uuden keinon henkilötietojen suojan toteuttamisen varmistamiseksi. On ilmeistä, että osoitusvelvollisuus edellyttää rekisterinpitäjiltä uudenlaista suhtautumistapaa tietosuojalainsäädännön asettamiin edellytyksiin. Parhaimmassa tapauksessa osoitusvelvollisuus saattaakin lisätä rekisterinpitäjien tietosuojaymmärrystä ja johtaa tehokkaampien, käsittelytoimille tilannekohtaisesti sopivien suojakeinojen käyttöönottoon ja henkilötietojen suojan tehokkaampaan toteutumiseen. Jääkin nähtäväksi, tuoko osoitusvelvollisuus tietosuojan teoriasta käytäntöön.